

# Change 1 (Aug '21)

## SMARTupdate to CYBER1

### CYBER1: The Cyberspace Operations & Electronic Warfare SMARTbook

\* **SMARTupdate 1 to CYBER1 (Aug '21)** updates the first printing of the CYBER1 SMARTbook (Oct '19) by incorporating new material from FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), ATP 3-12.3, Electronic Warfare Techniques (Jul '19), ATP 6-02.70, Techniques for Spectrum Management Operations (Oct '19), JP 3-85, Joint Electromagnetic Spectrum Management Operations (May '20) and adding a new section on Cyberspace IPB (ATP 2-01.3, Jul '19). An asterisk marks changed pages.

#### SMARTupdate Instructions

- 1. Download or Purchase.** Download a FREE PDF copy or purchase ready to insert. Available at: [www.TheLightningPress.com/smartupdates](http://www.TheLightningPress.com/smartupdates).
- 2. Print the PDF Two-Sided.** Depending on your printer, print landscape as a booklet or portrait two-sided (printer settings and capabilities vary).
- 3. Cut/Trim and Hole-Punch.** A local print shop can trim your pages to 5.5" x 8.5" along the chapter bleed tabs, and hole-punch for GBC plastic-comb.
- 4. Switch-out/Insert Changed Pages.** Gently pull-apart your GBC plastic-comb and replace affected pages with the updated pages (marked w/asterisks).

To get the full scope of new material, doctrinal changes and edits fully incorporated throughout, we recommend readers upgrade to the *updated CYBER1-1: The Cyberspace Operations & Electronic Warfare SMARTbook (w/SMARTupdate 1 incorporated)*.

#### Keep your SMARTbooks Up-to-Date!

To check for the latest updates and to register for e-mail notification of future changes to your SMARTbooks, visit [www.TheLightningPress.com/smartupdates](http://www.TheLightningPress.com/smartupdates)

#### The Lightning Press



2227 Arrowhead Blvd  
Lakeland, FL 33813  
24-hour Voicemail/Fax/Order: 1-800-997-8827  
E-mail: [SMARTbooks@TheLightningPress.com](mailto:SMARTbooks@TheLightningPress.com)

[www.TheLightningPress.com](http://www.TheLightningPress.com)

ISBN 9781935886907



90000 >



9 781935 886907

# The Lightning Press



2227 Arrowhead Blvd.

Lakeland, FL 33813

**24-hour Voicemail/Fax/Order:** 1-800-997-8827

**E-mail:** SMARTbooks@TheLightningPress.com

**www.TheLightningPress.com**

## Change 1 (Aug '21) SMARTupdate to CYBER1

\* **SMARTupdate 1 to CYBER1 (Aug '21)** updates the first printing of the CYBER1 SMARTbook (Oct '19) by incorporating new material from FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), ATP 3-12.3, Electronic Warfare Techniques (Jul '19), ATP 6-02.70, Techniques for Spectrum Management Operations (Oct '19), JP 3-85, Joint Electromagnetic Spectrum Management Operations (May '20) and adding a new section on Cyberspace IPB (ATP 2-01.3, Jul '19). An asterisk marks changed pages.

**To get the full scope of new material, doctrinal changes and edits** fully incorporated throughout, we recommend readers upgrade to the *updated CYBER1-1: The Cyberspace Operations & Electronic Warfare SMARTbook (w/SMARTupdate 1 incorporated)*.

*\*Pages marked with asterisks represent changed/inserted pages.*

**Copyright © 2021 Norman M. Wade**

**ISBN: 978-1-935886-90-7**

### All Rights Reserved

No part of this book may be reproduced or utilized in any form or other means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval systems, without permission in writing by the publisher. Inquiries should be addressed to The Lightning Press.

### Notice of Liability

The information in this SMARTbook and quick reference guide is distributed on an "As Is" basis, without warranty. While every precaution has been taken to ensure the reliability and accuracy of all data and contents, neither the author nor The Lightning Press shall have any liability to any person or entity with respect to liability, loss, or damage caused directly or indirectly by the contents of this book. If there is a discrepancy, refer to the source document. This SMARTbook does not contain classified or sensitive information restricted from public release.

"The views presented in this publication are those of the author and do not necessarily represent the views of the Department of Defense or its components."

**SMARTbook is a trademark of The Lightning Press.**

**Photo Credits.** Photos courtesy Department of Defense and the Military Services.

**Printed and bound in the United States of America.**

View, download FREE samples and purchase online:

**www.TheLightningPress.com**



# (CYBER1-1) Notes to Reader

## The Cyberspace Operations & Electronic Warfare SMARTbook

United States armed forces operate in an increasingly **network-based world**. The proliferation of information technologies is changing the way humans interact with each other and their environment, including interactions during military operations. This broad and rapidly changing operational environment requires that today's armed forces must operate in cyberspace and leverage an **electromagnetic spectrum** that is increasingly competitive, congested, and contested.

**Cyberspace** is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Operations in cyberspace contribute to gaining a significant operational advantage for achieving military objectives.

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

**Cyberspace operations (CO)** are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace operations consist of three functions: offensive cyberspace operations, defensive cyberspace operations, and Department of Defense information network operations.

**Electromagnetic Warfare (EW)** is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three functions: electromagnetic attack, electromagnetic protection, and electromagnetic support.

**Spectrum management operations (SMO)** are the interrelated functions of spectrum management, frequency assignment, host-nation coordination, and policy that enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations.

**Department of Defense information network (DODIN) operations** are operations to secure, configure, operate, extend, maintain, and sustain DOD cyberspace.

**Cybersecurity** incorporates actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity on DOD information systems and computer networks.



## SMARTbooks - DIME is our DOMAIN!

SMARTbooks: Reference Essentials for the Instruments of National Power (D-I-M-E: Diplomatic, Informational, Military, Economic)! Recognized as a "whole of government" doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a comprehensive professional library.

SMARTbooks can be used as quick reference guides during actual operations, as study guides at education and professional development courses, and as lesson plans and checklists in support of training. Visit [www.TheLightningPress.com](http://www.TheLightningPress.com)!



# (CYBER1-1) References

---

The following references were used in part to compile "CYBER1: The Cyberspace Operations and Electronic Warfare SMARTbook." All military references used to compile SMARTbooks are in the public domain and are available to the general public through official public websites and designated as approved for public release with unlimited distribution. The SMARTbooks do not contain ITAR-controlled technical data, classified, or other sensitive material restricted from public release. SMARTbooks are reference books that address general military principles, fundamentals and concepts rather than technical data or equipment operating procedures.

**\* SMARTupdate 1 to CYBER1 (Aug '21)** updates the first printing of the CYBER1 SMARTbook (Oct '19) by incorporating new material from FM 3-12 (Aug '21), ATP 3-12.3 (Jul '19), ATP 6-02.70 (Oct '19), JP 3-85 (May '20) and adding a new section on Cyberspace IPB (ATP 2-01.3) An asterisk marks changed pages. (Learn more at [www.thelightningpress.com/smartupdates/](http://www.thelightningpress.com/smartupdates/))

## Joint Publications

JP 3-0	Oct 2018	Joint Operations (w/Change 1)
JP 3-12	Jun 2019	Cyberspace Operations
JP 3-13.1	Feb 2012	Electronic Warfare
JP 3-13	Nov 2014	Information Operations (with Change 1)
JP 3-85*	May 2020	Joint Electromagnetic Spectrum Management Operations

## Field Manuals (FMs) and Training Circulars (TCs)

FM 3-0	Dec 2017	Operations (with Change 1)
FM 3-12*	Aug 2021	Cyberspace Operations and Electromagnetic Warfare
FM 6-0	Apr 2016	Commander and Staff Organization and Operations (w/change 2*)

## Army Tactics, Techniques and Procedures (ATPs/ATTPs)

ATP 3-12.3*	Jul 2019	Electronic Warfare Techniques
ATP 6-02.70*	Oct 2019	Techniques for Spectrum Management Operations
ATP 6-02.71	Apr 2019	Techniques for Department of Defense Information Network Operations
ATP 2-01.3*	Jan 2020	Intelligence Preparation of the Battlefield (w/Change 1)

## Other Publications

CSL (USAWC)	June 2017	Strategic Cyberspace Operations Guide
PAM 525-3-1	Dec 2018	The U.S. Army in Multi-Domain Operations 2028

*\* Denotes new/updated reference since first printing.*



# Cyberspace Operations

<b>I. Cyberspace and the Electromagnetic Spectrum.....</b>	<b>2-1*</b>
I. Cyberspace and the Electromagnetic Spectrum (EMS) .....	2-2*
Cyberspace Operations & Electromagnetic Warfare (EW) Logic Chart .....	2-3*
A. Operational Environment (OE) Overview.....	2-4*
- Operational Initiative .....	2-4*
- The Multi-Domain Extended Battlefield .....	2-4*
B. Cyberspace Domain .....	2-6*
- Physical Network Layer .....	2-6*
- Logical Network Layer .....	2-6*
- Cyber-Persona Layer.....	2-6*
C. Operational & Mission Variables.....	2-8*
III. Trends and Characteristics .....	2-10*
A. Congested Environments.....	2-10*
B. Contested Environments.....	2-10*
C. Threats.....	2-10*
D. Hazards .....	2-11*
III. Core Competencies & Fundamentals.....	2-12*
A. Core Competencies .....	2-12*
B. Fundamental Principles .....	2-12*
IV. Contributions to the Warfighting Functions.....	2-14*
V. Conflict and Competition .....	2-16*
A. Competition Continuum .....	2-16*
B. Multi-Domain Extended Battlefield.....	2-16*
C. Positions of Relative Advantage (in Cyberspace and the EMS) .....	2-16*
<b>II. Cyberspace Operations .....</b>	<b>2-17*</b>
Electromagnetic Spectrum Superiority .....	2-17*
I. Cyberspace Operations .....	2-17*
Cyberspace Operations (Missions & Actions) Overview .....	2-19*
A. Department of Defense Information Network Operations (DODIN) .....	2-18*
B. Defensive Cyberspace Operations (DCO).....	2-18*
- Defensive Cyberspace Operations Internal Defensive Measures (DCO-IDM) .....	2-20*
- Defensive Cyberspace Operations Response Action (DCO-RA).....	2-20*
C. Offensive Cyberspace Operations (OCO) .....	2-20*
II. Cyberspace Actions .....	2-21*
A. Cyberspace Security .....	2-21*
B. Cyberspace Defense .....	2-21*
C. Cyberspace Exploitation.....	2-21*
D. Cyberspace Attack.....	2-22*
III. Interrelationship with Other Operations .....	2-23*
A. Intelligence Operations .....	2-23*
B. Space Operations .....	2-24*
C. Information Operations (IO) .....	2-25*
<b>III. Army Organizations &amp; Command and Control .....</b>	<b>2-27*</b>
I. United States Army Cyber Command.....	2-27*
II. Army Information Warfare Operations Center .....	2-27*
III. Cyberspace Electromagnetic Activities at Corps and Below .....	2-28*
A. Commander's Role .....	2-28*
B. Cyberspace Electromagnetic Activities (CEMA) Section .....	2-29*

- Cyber Electromagnetic Warfare Officer (CEWO).....	2-30*
- Cyber Warfare Officer or Cyber-Operations Officer.....	2-31*
- Electromagnetic Warfare Technician (EWT).....	2-31*
- Electromagnetic Warfare Sergeant Major or NCOIC.....	2-31*
- Electromagnetic Warfare Noncommissioned Officer (EW NCO).....	2-31*
- Cyberspace Electromagnetic Activities Spectrum Manager.....	2-31*
C. Cyberspace Electromagnetic Activities (CEMA) Working Group.....	2-29*
IV. Staff and Support at Corps and Below.....	2-32*
A. Assistant Chief of Staff, Intelligence.....	2-32*
B. Assistant Chief of Staff, Signal.....	2-33*
C. G-6 or S-6 Spectrum Manager.....	2-34*
D. Information Operations Officer or Representative.....	2-34*
E. Fires Support Element.....	2-34*
F. Staff Judge Advocate.....	2-34*
V. Electromagnetic Warfare (EW) Organizations.....	2-36*
Electromagnetic Warfare (EW) Platoon.....	2-36*
Intelligence, Information, Cyber, EW, & Space (I2CEWS).....	2-36*
<b>IV. Integration through the Operations Process.....</b>	<b>2-37*</b>
I. The Operations Process.....	2-37*
A. Planning.....	2-38*
B. Preparation.....	2-38*
C. Execution.....	2-39*
D. Assessment.....	2-39*
II. Integrating Processes.....	2-40*
A. Intelligence Preparation of the Battlefield (IPB).....	2-40*
B. Information Collection.....	2-40*
C. Targeting.....	2-41*
D. Risk Management.....	2-41*
E. Knowledge Management.....	2-41*
III. Risks In Cyberspace and the EMS.....	2-42*
A. Operational Risks.....	2-42*
B. Technical Risks.....	2-42*
C. Policy Risks.....	2-43*
D. Operations Security Risks.....	2-43*

# Electromagnetic Warfare (EW)

<b>I. Electromagnetic Warfare (EW).....</b>	<b>3-1*</b>
I. Electromagnetic Warfare (EW) ( <i>Note about change in terms</i> ).....	3-1*
A. Electromagnetic Attack (EA).....	3-2*
- Offensive EA.....	3-2*
- Defensive EA.....	3-2*
- Electromagnetic Attack (EA) Effects.....	3-2*
- Electromagnetic Attack (EA) Tasks.....	3-3*
B. Electromagnetic Protection (EP).....	3-6*
- Electromagnetic Protection Tasks.....	3-6*
C. Electromagnetic Support (ES).....	3-8*
- Electromagnetic Support Tasks.....	3-8*
- Electromagnetic Support (ES) Actions.....	3-9*
* Electromagnetic Warfare Reprogramming.....	3-8*

III. Spectrum Management .....	3-10*
- Electromagnetic Interference (EMI) .....	3-10*
- Frequency Interference Resolution .....	3-10*
- Spectrum Management Operations (SMO).....	3-10*
- Electromagnetic Warfare Coordination .....	3-10*
<b>II. EW Key Personnel.....</b>	<b>3-11*</b>
I. Electronic Warfare Personnel .....	3-11*
II. Theater Army, Corps, Division and Brigade.....	3-11*
A. Cyber Electronic Warfare Officer (CEWO).....	3-12*
B. Electronic Warfare Technician.....	3-12*
C. Electronic Warfare Noncommissioned Officer .....	3-13*
D. Spectrum Manager .....	3-13*
E. Battalion Electronic Warfare Personnel .....	3-13*
F. Company CREW Specialists .....	3-16*
G. Electronic Warfare Control Authority .....	3-16*
III. Staff Members and Electronic Warfare .....	3-14*
<b>III. EW Preparation &amp; Execution .....</b>	<b>3-17*</b>
I. Electronic Warfare Preparation.....	3-17*
II. Integration of Electronic Warfare and Signals Intelligence .....	3-18*
Deconflicting the Electromagnetic Spectrum.....	3-19*
A. Distinctions Between Electronic Warfare and Signals Intelligence .....	3-18*
B. Sensing Activity Distinctions .....	3-18*
III. Electronic Warfare Execution .....	3-20*
<b>IV(a). Electronic Attack Techniques.....</b>	<b>3-21*</b>
I. Planning Electronic Attack .....	3-21*
A. Electronic Attack Effects .....	3-21*
B. Electronic Attack (EA) Considerations .....	3-22*
II. Preparing Electronic Attack.....	3-24*
- Electronic Attack Requests (EARFs).....	3-25*
- Electronic Attack Considerations.....	3-24*
III. Executing Electronic Attack .....	3-24*
Close Air Support (CAS).....	3-24*
A. Airborne Electronic Attack .....	3-26*
B. Defensive Electronic Attack .....	3-28*
- Counter Radio-Controlled Improvised Device (CREW).....	3-28*
IV. Electronic Attack Techniques in Large Scale Combat Operations .....	3-28*
<b>IV(b). Electronic Protection Techniques.....</b>	<b>3-29*</b>
I. Planning Electronic Protection.....	3-29*
Electronic Protection Considerations .....	3-30*
II. Electromagnetic Interference.....	3-31*
A. Recognizing Electromagnetic Jamming.....	3-31*
B. Remedial Electronic Protection Techniques.....	3-32*
C. Concealment.....	3-32*
D. Threat Electronic Attack on Friendly Command Nodes .....	3-32*
E. Electromagnetic Interference (EMI) Battle Drill.....	3-33*
III. Staff Electronic Protection Responsibilities .....	3-34*
IV. Equipment and Communications Enhancements.....	3-34*
<b>IV(c). Electronic Warfare Support Techniques.....</b>	<b>3-35*</b>
I. Planning Electronic Warfare Support.....	3-35*
A. Electronic Reconnaissance.....	3-35*
B. Electronic Warfare Support Considerations .....	3-35*
II. Preparing Electronic Warfare Support .....	3-35*
A. Electromagnetic Environment (EME) Survey.....	3-36*
B. Direction Finding (DF).....	3-36*

# Cyberspace & EW (CEMA) Planning

<b>IPB Cyberspace Considerations.....</b>	<b>4-a*</b>
Intelligence Preparation of the Battlefield (IPB).....	4-a*
Step 1 — Define the Operational Environment.....	4-b*
A. Step 1 Cyberspace Considerations .....	4-b*
B. Cyber-Centric Activities and Outputs for Step 1.....	4-d*
Step 2 — Describe Environmental Effects on Operations.....	4-e*
A. Step 2 Cyberspace Considerations .....	4-e*
B. Cyber-Centric Activities & Outputs for Step 2 .....	4-f*
Threat Overlay .....	4-f*
Threat Description Table .....	4-f*
Modified Combined Obstacle Overlay .....	4-g*
Terrain Effects Matrix .....	4-h*
Weather, Light, and Illumination Charts or Tables .....	4-h*
Civil Considerations Data Files, Overlays, and Assessments.....	4-h*
Step 3 — Evaluate the Threat .....	4-i*
A. Step 3 Cyberspace Considerations .....	4-j*
B. Cyber-Centric Activities and Outputs for Step 3.....	4-j*
Threat Characteristics.....	4-k*
Threat Model.....	4-l*
- Cyber Kill Chain .....	4-l*
- Threat Tactics, Options, and Peculiarities.....	4-m*
- High-Value Targets .....	4-m*
Threat Capabilities .....	4-k*
Step 4 — Determine Threat Courses of Action.....	4-n*
A. Step 4 Cyberspace Considerations .....	4-n*
B. Cyber-Centric Activities and Outputs for Step 4.....	4-n*
Threat Situation Template .....	4-o*
Event Template .....	4-p*
Event Matrix.....	4-q*
<b>I(a). Cyberspace (CEMA) Operations Planning.....</b>	<b>4-1</b>
I. Army Design Methodology.....	4-2
II. The Military Decision-Making Process (MDMP) .....	4-2
- Step 1: Receipt of Mission .....	4-2
- Step 2: Mission Analysis .....	4-3
- Step 3: Course of Action Development .....	4-4
- Step 4: Course of Action Analysis .....	4-5
- Step 5: Course of Action Comparison .....	4-6
- Step 6: Course of Action Approval .....	4-7
- Step 7: Orders Production, Dissemination, and Transition .....	4-8
<b>I(b). Cyber Effects Request Format (CERF) .....</b>	<b>4-9</b>
I. Requesting Cyberspace Effects .....	4-9
- Cyber Effects Request Format (CERF).....	4-11
II. Cyber Effects Request Format Preparation.....	4-12
<b>II(a). Electronic Warfare Planning .....</b>	<b>4-15*</b>
I. Electronic Warfare Contributions to the Military Decision-Making Process .....	4-15*
II. Electronic Warfare Planning Considerations .....	4-15*
A. Planning Factors .....	4-15*
Electronic Warfare Running Estimate .....	4-16*

III. Staff Contributions to EW Planning .....	4-19*
EW Contributions to the Staff .....	4-20*
Joint Restricted Frequency List (JRFL) .....	4-22*
III. Electronic Warfare Configurations .....	4-23*
V. EW Employment Considerations .....	4-24*
VI. Electronic Warfare Assessment .....	4-26*
<b>II(b). Electromagnetic Attack Request.....</b>	<b>4-27*</b>
I. Electromagnetic Attack Request.....	4-27*
II. Airborne Electromagnetic Attack Support .....	4-28*
<b>III. Targeting (D3A).....</b>	<b>4-29*</b>
Targeting Methodology .....	4-30*
Targeting Crosswalk .....	4-31*
I. Decide.....	4-32*
II. Detect .....	4-33*
III Deliver.....	4-33*
IV. Assess .....	4-33*
Considerations When Targeting.....	4-34*
<b>IV. Cyberspace (CEMA) in Operations Orders .....</b>	<b>4-35*</b>
- ANNEX C—OPERATIONS (G-5 OR G-3 [S-3]) .....	4-35*
- ANNEX H—SIGNAL (G-6 [S-6]).....	4-35*
- Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C.....	4-35*
(Operations) to Operations Plans and Orders	
- Appendix 12 to Annex C (Sample Format).....	4-36*
<b>V. Cyberspace Integration into Joint Planning (JPP).....</b>	<b>4-41</b>
I. Cyberspace Planning Integration.....	4-42
II. Cyberspace Planning and the JPP .....	4-42
A. Initiation.....	4-42
B. Mission Analysis.....	4-42
C. Course of Action (COA) Development .....	4-43
D. COA Analysis, Comparison, and Approval.....	4-43
E. Plan or Order Development .....	4-43
IV. Cyberspace-Related Intelligence Requirements (IRs) .....	4-44
V. Information Operations (IO).....	4-44
VI. Planning Insights .....	4-44
<b>VI. Integrating / Coordinating Functions of IO.....</b>	<b>4-45</b>
I. Information Operations and the Information-Influence .....	4-45
Relational Framework	
II. The Information Operations Staff and Information Operations Cell.....	4-46
III. Relationships and Integration .....	4-46
- Commander's Communication Synchronization (CCS) .....	4-46
A. Strategic Communication (SC) .....	4-46
B. Joint Interagency Coordination Group (JIACG) .....	4-47
C. Public Affairs (PA) .....	4-48
D. Civil-Military Operations (CMO).....	4-48
E. Cyberspace Operations .....	4-48
F. Information Assurance (IA) .....	4-49
G. Space Operations.....	4-49
H. Military Information Support Operations (MISO).....	4-49
I. Intelligence .....	4-49
J. Military Deception (MILDEC).....	4-49
K. Operations Security (OPSEC) .....	4-50
L. Special Technical Operations (STO) .....	4-50
M. Joint Electromagnetic Spectrum Operations (JEMSO) .....	4-50
N. Key Leader Engagement (KLE).....	4-50

# Spectrum Management Operations (SMO/JEMSO)

<b>I. Spectrum Management Operations (SMO/JEMSO).....</b>	<b>5-1*</b>
I. Electromagnetic Spectrum Operations (EMSO).....	5-1*
Electromagnetic Operational Environment (EMOE).....	5-2*
- Electromagnetic Spectrum (EMS) .....	5-2*
- Electromagnetic Environment (EME).....	5-2*
II. Spectrum Management Operations (SMO).....	5-4*
A. Objective of Spectrum Management Operations.....	5-5*
B. Spectrum Management Operations Core Functions.....	5-5*
III. Joint Electromagnetic Spectrum Operations (JEMSO).....	5-5*
A. JEMSO Actions .....	5-6*
- Exploitation .....	5-6*
- Electronic Attack (EA) .....	5-6*
- Protect .....	5-6*
- Manage.....	5-7*
B. Electromagnetic Environmental Effects (E3) .....	5-8*
- HERP.....	5-8*
- HERO .....	5-8*
- HERF.....	5-8*
- Electromagnetic Pulse (EMP).....	5-8*
- High-Altitude Electromagnetic Pulse (HEMP).....	5-8*
<b>II. Spectrum Management.....</b>	<b>5-9*</b>
Frequency Interference Resolution.....	5-9*
I. Key SMO inputs to the MDMP.....	5-10*
II. SMO Support to the Warfighting Functions .....	5-12*
II. The Common Operational Picture (COP).....	5-14*
- Live Spectrum Analysis.....	5-14*
- Movement of Forces to a New Location.....	5-14*
<b>III. Planning Joint EMS Operations (JEMSO).....</b>	<b>5-15*</b>
Planning Process.....	5-15*
JEMSMO Cell Actions and Outputs as Part of Joint Planning.....	5-17*
Information (Planning Considerations) .....	5-18*
I. Electromagnetic Order of Battle (EOB).....	5-15*
II. EMOE Estimate .....	5-16*
III. JEMSO Staff Estimate .....	5-20*
- EMS Superiority Approach.....	5-20*
- Determine Friendly EMS-Use Requirements .....	5-20*
IV. JEMSO Appendix to Annex C.....	5-20*



# Introduction (Threat/COE/Info)

United States armed forces operate in an increasingly network-based world. The proliferation of information technologies is changing the way humans interact with each other and their environment, including interactions during military operations. This broad and rapidly changing operational environment requires that today's armed forces must operate in cyberspace and leverage an electromagnetic spectrum that is increasingly competitive, congested, and contested.

## Cyberspace

Cyberspace reaches across geographic and geopolitical boundaries and is integrated with the operation of critical infrastructures, as well as the conduct of commerce, governance, and national defense activities. Access to the Internet and other areas of cyberspace provides users operational reach and the opportunity to compromise the integrity of critical infrastructures in direct and indirect ways without a physical presence. The prosperity and security of our nation are significantly enhanced by our use of cyberspace, yet these same developments have led to increased exposure of vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular.

*See pp. 1-1 to 1-6 and 2-1 to 2-16*

## Cyberspace Operations (CO)

Cyberspace Operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO comprise the military, national intelligence, and ordinary business operations of DOD in and through cyberspace. Although commanders need awareness of the potential impact of the other types of DOD CO on their operations, the military component of CO is the only one guided by joint doctrine and is the focus of this publication. CCDRs and Services use CO to create effects in and through cyberspace in support of military objectives. Military operations in cyberspace are organized into missions executed through a combination of specific actions that contribute to achieving a commander's objective.

*See pp. 1-15 and 2-17.*

## Electromagnetic Warfare (EW)\*

Electromagnetic Warfare (EW) is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three functions: electromagnetic attack, electromagnetic protection, and electromagnetic support.

*\* Editor's Note: In keeping with doctrinal terminology changes in JP 3-85, Joint Electromagnetic Spectrum Operations (May '20) and FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), the term "electronic warfare (EW)" has been updated to "electromagnetic warfare (EW)". Likewise, the EW divisions have been updated as "electromagnetic attack (EA), electromagnetic protection (EP), and electromagnetic support (ES)." For purposes of the CYBER1 SMARTbook, EW/EA/EP/ES acronyms and terms will remain the same as presented in the original cited and dated source -- for example, ATP 3-12.3, Electronic Warfare Techniques (Jul '19). Readers should anticipate that as those specific references are updated/revised, so will the terms.*

# I. The Global Cyber Threat

*Ref: Daniel R. Coats, Director Of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community (Jan 29, 2019).*

Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.

At present, China and Russia pose the greatest espionage and cyber attack threats, but we anticipate that all our adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities into their efforts to influence US policies and advance their own national security interests. In the last decade, our adversaries and strategic competitors have developed and experimented with a growing capability to shape and alter the information and systems on which we rely. For years, they have conducted cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk. They are now becoming more adept at using social media to alter how we think, behave, and decide. As we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic competitors almost certainly will gain greater insight into and access to our protected information.

## China

China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies. It is improving its cyber attack capabilities and altering information online, shaping Chinese views and potentially the views of US citizens—an issue we discuss in greater detail in the Online Influence Operations and Election Interference section of this report.

- Beijing will authorize cyber espionage against key US technology sectors when doing so addresses a significant national security or economic goal not achievable through other means. We are also concerned about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies.
- China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.

## Russia

We assess that Russia poses a cyber espionage, influence, and attack threat to the United States and our allies. Moscow continues to be a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve its political and military objectives. Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat—an issue discussed in the Online Influence Operations and Election Interference section of this report.

# VI. Information Operations (IO)

Ref: JP 3-0, Joint Operations, w/Chg 1 (Oct '18), pp. III-17 to III-22.

All military activities produce **information**. Informational aspects are the features and details of military activities observers interpret and use to assign meaning and gain understanding. Those aspects affect the perceptions and attitudes that drive behavior and decision making. The JFC leverages informational aspects of military activities to gain an advantage; failing to leverage those aspects may cede this advantage to others. Leveraging the informational aspects of military activities ultimately affects strategic outcomes.

The **information function** encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making.

The **instruments of national power** (diplomatic, informational, military, and economic) provide leaders in the US with the means and ways of dealing with crises around the world. Employing these means in the information environment requires the ability to securely transmit, receive, store, and process information in near real time. The nation's state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities (IRCs) to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments. As the strategic environment continues to change, so does information operations (IO).

Regardless of its mission, the joint force considers the likely impact of all operations on **relevant actor** perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation in ways that **create desired effects** that include maintaining or inducing relevant actor behaviors. These ways may include the timing, duration, scope, scale, and even visibility of an operation; the deliberately planned presence, posture, or profile of assigned or attached forces in an area; the use of signature management in deception operations; the conduct of activities and operations to similarly impact behavioral drivers; and the **employment of specialized capabilities** -- e.g., key-leader engagements (KLE), cyberspace operations (CO), military information support operations (MISO), electronic warfare (EW), and civil affairs (CA) -- to reinforce the JFC's efforts.

**Inform activities** involve the release of accurate information to domestic and international audiences to put joint operations in context; facilitate informed perceptions about military operations; and counter adversarial misinformation, disinformation, and propaganda. Inform activities help to assure the trust and confidence of the US population, allies, and partners and to deter and dissuade adversaries and enemies.

The joint force **attacks and exploits information, information networks, and systems** to affect the ability of relevant actors to leverage information in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.



Refer to INFO1: The Information Operations & Capabilities SMARTbook (Guide to Information Operations & the IRCs). See following pages (pp. 0-11a to 0-11b) for an overview of this companion book to the CYBER1 SMARTbook.

See pp. 4-45 to 4-50 for discussion of the the integrating/coordinating functions of information operations (IO) and pp. 4-51 to 4-54 for related discussion of IO planning.



# INFO1: The Information Operations & Capabilities SMARTbook

## Guide to Information Operations & the IRCs

Over the past two decades, information operations (IO) has gone through a number of doctrinal evolutions, explained, in part, by the rapidly changing nature of information, its flow, processing, dissemination, impact and, in particular, its military employment. INFO1: The Information Operations & Capabilities SMARTbook examines the most current doctrinal references available and charts a path to emerging doctrine.



FM 3-13



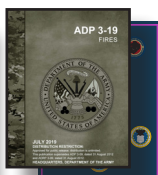
ATP 3-13.1



JP 3-13 (Chg 1)



JP 3-0 (Chg 1)



Plus more than a dozen primary references on the IRCs and more!

INFO1 chapters and topics include information operations (IO defined and described), information in joint operations (joint IO), information-related capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution (IO working group, IO weighted efforts and enabling activities, intel support), fires & targeting, and information assessment.

## Chap 1: Information Operations (Defined & Described)

**Information** is a resource. As a resource, it must be obtained, developed, refined, distributed, and protected. The **information element of combat power** is integral to optimizing combat power, particularly given the increasing relevance of operations in and through the information environment to achieve decisive outcomes.

**Information Operations (IO)** is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. The purpose of IO is to **create effects in and through the information environment** that provide commanders decisive advantage over enemies and adversaries.

## Chap 2: Information in Joint Operations

The joint force commander (JFC) **leverages informational aspects of military activities to gain an advantage**; failing to leverage those aspects may cede this advantage to others. Leveraging the informational aspects of military activities ultimately affects strategic outcomes. The joint force **attacks and exploits information, information networks, and systems to affect the ability of relevant actors to leverage information** in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.

## Chap 3: Information-Related Capabilities (IRCs)

An **information-related capability (IRC)** is a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. IO brings together information-related capabilities (IRCs) at a specific time and in a coherent fashion to create effects in and through the information environment that advance the ability to deliver operational advantage to the commander.

All unit operations, activities, and actions affect the information environment. Even if they primarily affect the physical dimension, they nonetheless also affect the informational and cognitive dimensions. For this reason, whether or not they are routinely considered an IRC, a wide variety of unit functions and activities can be adapted for the purposes of conducting information operations or serve as enablers to its planning, execution, and assessment.

## Chap 4: Information Planning

**Planning** is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. Commanders, supported by their staffs, ensure IO is fully integrated into the plan, starting with Army design methodology (ADM) and progressing through the military decisionmaking process (MDMP). The focal point for IO planning is the IO officer (or designated representative for IO). However, the entire staff contributes to planning products that describe and depict how IO supports the commander's intent and concept of operations.

## Chap 5: Information Planning

**Preparation** consists of those activities performed by units and Soldiers to improve their ability to execute an operation. Preparation creates conditions that improve friendly force opportunities for success. Because many IO objectives and IRC tasks require long lead times to create desired effects, preparation for IO often starts earlier than for other types of operations. Initial preparation for specific IRCs and IO units (such as 1st IO Command or a Theater IO Group) may begin during peacetime.

## Chap 6: Information Execution

**Execution** of IO includes IRCs executing the synchronization plan and the commander and staff monitoring and assessing their activities relative to the plan and adjusting these efforts, as necessary. The primary mechanism for monitoring and assessing IRC activities is the **IO working group**. There are two variations of the IO working group. The first monitors and assesses ongoing planned operations and convenes on a routine, recurring basis. The second monitors and assesses unplanned or crisis situations and convenes on an as-needed basis.

## Chap 7: Fires & Targeting

The **fires warfighting function** is the related tasks and systems that **create and converge effects in all domains** against the threat to enable actions across the range of military operations. These tasks and systems create **lethal and nonlethal effects** delivered from both Army and Joint forces, as well as other unified action partners.

**Targeting** is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). IO is integrated into the targeting cycle to produce effects in and through the information environment that support objectives.

## Chap 8: Information Assessment

**Assessment** precedes and guides the other activities of the operations process. It is also part of targeting. In short, assessment occurs at all levels and within all operations and has a role in any process or activity. The purpose of assessment is to improve the commander's decision making and make operations more effective. Assessment is a key component of the commander's decision cycle, helping to determine the results of unit actions in the context of overall mission objectives.

# Information Function Activities

Ref: JP 3-0, *Joint Operations*, w/Chg 1 (Oct '18), pp. III-17 to III-22.

The information function includes activities that facilitate the JFC's understanding of the role of information in the OE, facilitate the JFC's ability to leverage information to affect behavior, and support human and automated decision making.

## 1. Understand Information in the Operational Environment (OE)

In conjunction with activities under the intelligence joint function, this activity facilitates the JFC's understanding of the pervasive nature of information in the OE, its impact on relevant actors, and its effect on military operations. It includes determining relevant actor perceptions, attitudes, and decision-making processes and requires an appreciation of their culture, history, and narratives, as well as knowledge of the means, context, and established patterns of their communication.

Information affects the perceptions and attitudes that drive the behavior and decision making of humans and automated systems. In order to affect behavior, the JFC must understand the perceptions, attitudes, and decision-making processes of humans and automated systems. These processes reflect the aggregate of social, cultural, and technical attributes that act upon and impact knowledge, understanding, beliefs, world views, and actions.

The human and automated systems whose behavior the JFC wants to affect are referred to as relevant actors. Relevant actors may include any individuals, groups, and populations, or any automated systems, the behavior of which has the potential to substantially help or hinder the success of a particular campaign, operation, or tactical action. For the purpose of military activities intended to inform audiences, relevant actors may include US audiences; however, US audiences are not considered targets for influence.

See pp. 0-6 to 0-9 for related discussion of the operational environment.

### Language, Regional, and Cultural Expertise

Language skills, regional knowledge, and cultural awareness enable effective joint operations. Deployed joint forces should understand and effectively communicate with HN populations; local and national government officials; multinational partners; national, regional, and international media; and other key stakeholders, including NGOs. This capability includes knowledge about the human aspects of the OE and the skills associated with communicating with foreign audiences. Knowledge about the human aspects of the OE is derived from the analysis of national, regional, and local culture, economy, politics, religion, and customs. Consequently, commanders should integrate training and capabilities for foreign language and regional expertise in contingency, campaign, and supporting plans and provide for them in support of daily operations and activities. Commanders should place particular emphasis on foreign language proficiency in technical areas identified as key to mission accomplishment.

For specific planning guidance and procedures regarding language and regional expertise, refer to CJCSI 3126.01, *Language, Regional Expertise, and Culture (LREC) Capability Identification, Planning, and Sourcing*.

## 2. Leverage Information to Affect Behavior

Tasks aligned under this activity apply the JFC's understanding of the impact information has on perceptions, attitudes, and decision-making processes to affect the behaviors of relevant actors in ways favorable to joint force objectives.



# I. Cyberspace and the Electromagnetic Spectrum

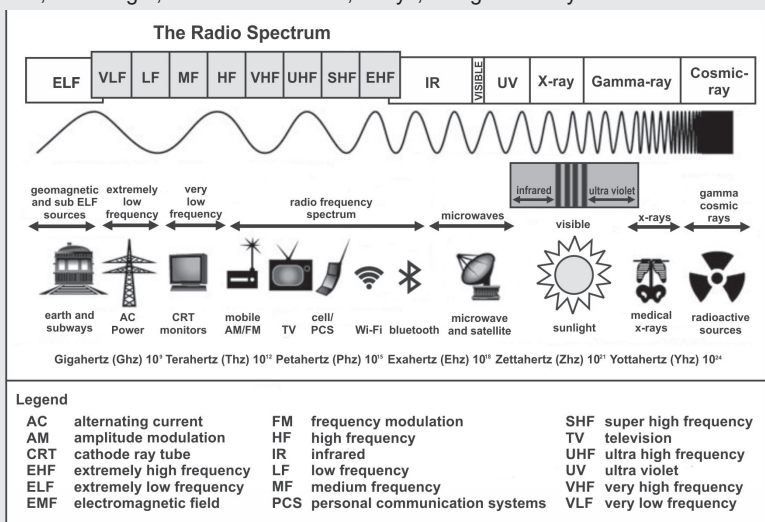
Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), chap. 1.

Cyberspace operations and electromagnetic warfare (EW) play an essential role in the Army's conduct of unified land operations as part of a joint force and in coordination with unified action partners. **Cyberspace operations** are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). **Electromagnetic warfare (EW)** is a military action involving the use of electromagnetic and directed energy to control the **electromagnetic spectrum** or to attack the enemy (JP 3-85).

See pp. 2-17 to 2-26 for discussion of *cyberspace operations* and chap. 3 for discussion of *electromagnetic warfare (EW)*.

## Electromagnetic Spectrum (EMS)

The electromagnetic spectrum (EMS) is a maneuver space essential for facilitating control within the operational environment (OE) and impacts all portions of the OE and military operations. Based on specific physical characteristics, the EMS is organized by frequency bands, including radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, x-rays, and gamma rays.



Ref: FM 3-12 (Aug '21), fig. 1-3. *The electromagnetic spectrum*. See also p. 5-2.

Cyberspace is one of the five domains of warfare and uses a portion of the electromagnetic spectrum (EMS) for operations, for example, Bluetooth, Wi-Fi, and satellite transport. Therefore, cyberspace operations and EW require frequency assignment, management, and coordination performed by spectrum management operations.

**Spectrum management operations** consist of four key functions—spectrum management, frequency assignment, host-nation coordination, and policy adherence. Spectrum management operations include preventing and mitigating frequency conflicts and electromagnetic interference (EMI) between friendly forces and host nations during Army operations. See chap. 5, *Spectrum Management Operations*.

## Cyberspace Operations

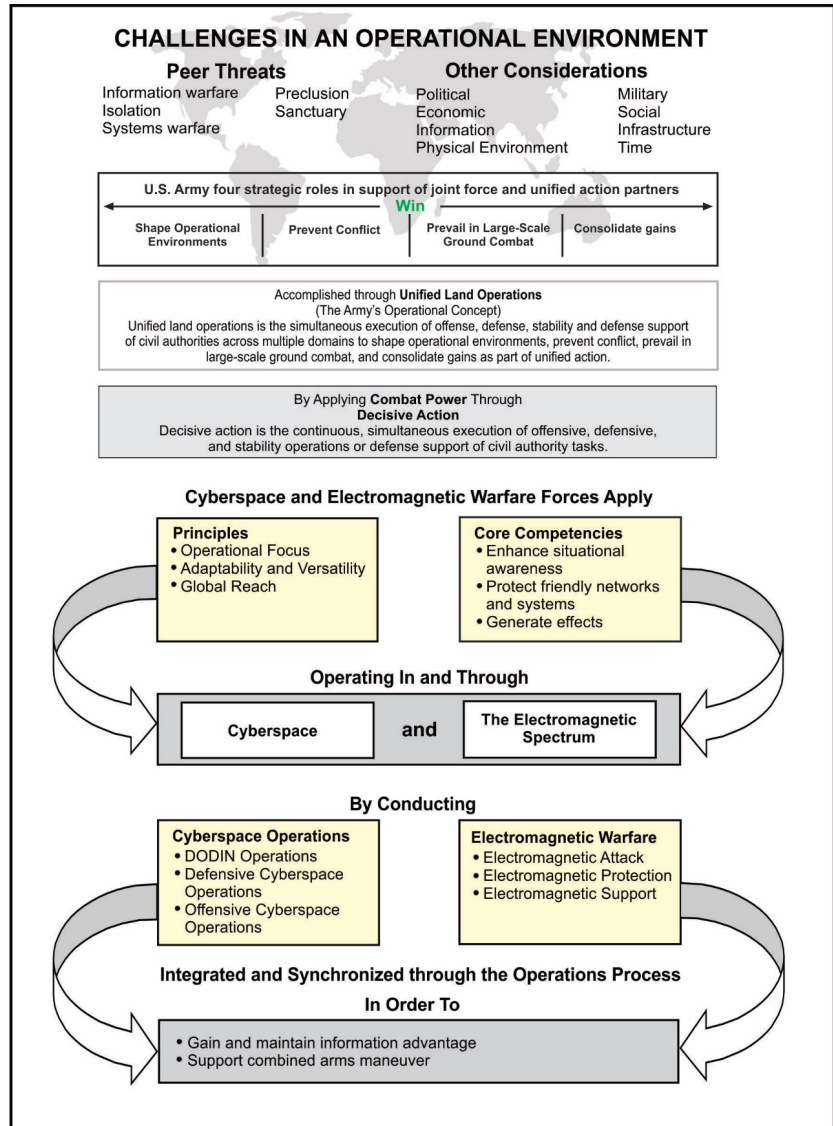
Commanders must leverage cyberspace and EW capabilities using a combined arms approach to seize, retain, and exploit the operational initiative. Effective use of cyberspace operations and EW require commanders and staffs to conduct cyberspace electromagnetic activities (CEMA). Cyberspace electromagnetic activities is the process of planning, integrating, and synchronizing cyberspace operations and electromagnetic warfare in support of unified land operations (ADP 3-0). By integrating and synchronizing cyberspace operations and EW, friendly forces gain an information advantage across multiple domains and lines of operations.

Army's reliance on networked systems and weapons necessitates highly trained forces to protect warfighting systems and networks dependent upon access to cyberspace and the EMS. Cyberspace and the EMS are heavily congested due to the high volume of friendly, neutral, and adversary use, and contested due to adversary actions.



# Cyberspace Operations & Electromagnetic Warfare (EW) Logic Chart

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), fig. 1-1.



# A. Operational Environment (OE) Overview

*Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), pp. 1-4 to 1-5.*

An **operational environment** is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Conditions in cyberspace and the EMS often change rapidly and can positively or negatively impact a commander's ability to achieve mission objectives. Friendly, neutral, adversary, and enemy actions in cyberspace and the EMS can create near-instantaneous effects on the battlefield or in garrison. Given the global nature of cyberspace and the EMS, these actions can impact a commander's OE even though the actions may originate or terminate beyond that OE. Cyberspace and EW effects also cross through and impact multiple domains simultaneously. For these reasons, commanders must gain and maintain an in-depth understanding of the OE that extends beyond the land domain to the multi-domain extended battlefield to seize, exploit, and retain operational initiative.

## Operational Initiative

Operational initiative is the setting of tempo and terms of action throughout an operation (ADP 3-0). By gaining and maintaining positions of relative advantage, including information advantage in and through cyberspace and the EMS, commanders can seize and retain the operational initiative. To gain and maintain information advantage, commanders must account for the temporal nature of information and the temporary nature of many cyberspace and EW effects. On average, the relative operational advantage that a commander can gain from a piece of information or from a cyberspace or EW effect degrades over time. This means that a commander who takes action first, on average, will obtain a greater information advantage from a similar piece of information or effect than a commander who acts later. In this way, the commander who can sense, understand, decide, act, and assess faster than an opponent will generally obtain the greatest information advantage.

Commanders can use cyberspace and EW capabilities to gain enhanced situational awareness and understanding of the enemy through reconnaissance and sensing activities. These reconnaissance and sensing activities can augment and enhance the understanding a commander gains from information collection and intelligence processes. Commanders can also use cyberspace and EW capabilities to decide and act faster than an adversary or enemy. By protecting friendly information systems and signals from disruption or exploitation by an adversary or enemy, a commander can ensure command and control and maintain tactical and operational surprise. Conversely, a commander might use cyberspace and EW capabilities to slow or degrade an enemy's decision-making processes by disrupting enemy sensors, communications, or data processing. To make effective use of cyberspace and EW capabilities to achieve an information advantage, a commander must plan early to integrate cyberspace operations and EW actions fully into the overall scheme of maneuver.

*See following pages (pp. 2-6 to 2-7) for discussion of the cyberspace domain.*

## The Multi-Domain Extended Battlefield

*Ref: FM 3-0, Operations (Oct '17), pp. 1-6 to 1-8.*

The interrelationship of the air, land, maritime, space, and the information environment (including cyberspace) requires a cross-domain understanding of an OE. Commanders and staffs must understand friendly and enemy capabilities that reside in each domain. From this understanding, commanders can better identify windows of opportunity during operations to converge capabilities for best effect. Since many friendly capabilities are not

organic to Army forces, commanders and staffs plan, coordinate for, and integrate joint and other unified action partner capabilities in a multi-domain approach to operations.

A **multi-domain approach** to operations is not new. Army forces have effectively integrated capabilities and synchronized actions in the air, land, and maritime domains for decades. Rapid and continued advances in technology and the military application of new technologies to the space domain, the EMS, and the information environment (particularly cyberspace) require special consideration in planning and converging effects from across all domains.

*See p. 2-16 for further discussion. Refer to TRADOC PAM 525-3-1, The U.S. Army in Multi-Domain Operations (Dec '18) for further discussion.*

## Information Environment

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). The information environment is not separate or distinct from the OE but is inextricably part of it. Any activity that occurs in the information environment simultaneously occurs in and affects one or more of the physical domains. Most threat forces recognize the importance of the information environment and emphasize information warfare as part of their strategic and operational methods.

The information environment is comprised of three dimensions: physical, informational, and cognitive. The physical dimension includes the connective infrastructure that supports the transmission, reception, and storage of information.

Across the globe, information is increasingly available in near-real time. The ability to access this information, from anywhere, at any time, broadens and accelerates human interaction across multiple levels, including person to person, person to organization, person to government, and government to government. Social media, in particular, enables the swift mobilization of people and resources around ideas and causes, even before they are fully understood. Disinformation and propaganda create malign narratives that can propagate quickly and instill an array of emotions and behaviors from anarchy to focused violence. From a military standpoint, information enables decision making, leadership, and combat power; it is also key to seizing, gaining, and retaining the initiative, and to consolidating gains in an OE. Army commanders conduct information operations to affect the information environment.

## Space Domain

The space domain is the space environment, space assets, and terrestrial resources required to access and operate in, to, or through the space environment (FM 3-14). Space is a physical domain like land, sea, and air within which military activities are conducted. Proliferation of advanced space technology provides more widespread access to space-enabled technologies than in the past. Adversaries have developed their own systems, while commercially available systems allow almost universal access to some level of space enabled capability with military applications. Army forces must be prepared to operate in a denied, degraded and disrupted space operational environment (D3SOE).

## Cyberspace and the Electromagnetic Spectrum (EMS)

Cyberspace is a global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace is an extensive and complex global network of wired and wireless links connecting nodes that permeate every domain. Networks cross geographic and political boundaries connecting individuals, organizations, and systems around the world. Cyberspace is socially enabling, allowing interactivity among individuals, groups, organizations, and nation-states.

*See following pages (pp. 2-6 to 2-7) for discussion of the cyberspace domain.*

## B. Cyberspace Domain

*Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), pp. 1-5 to 1-7. See pp. 1-2 to 1-3 for related discussion from JP 3-12.*

Cyberspace is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12). Cyberspace operations require the use of links and nodes located in other physical domains to perform logical functions that create effects in cyberspace that then permeate throughout the physical domains using both wired networks and the EMS.

The use of cyberspace is essential to operations. The Army conducts cyberspace operations and supporting activities as part of both Army and joint operations. Because cyberspace is a global communications and data-sharing medium, it is inherently joint, inter-organizational, multinational, and often a shared resource, with signal and intelligence maintaining significant equities. Friendly, enemy, adversary, and host-nation networks, communications systems, computers, cellular phone systems, social media websites, and technical infrastructures are all part of cyberspace.

To aid the planning and execution of cyberspace operations, cyberspace is sometimes visualized in three layers. These layers are interdependent, but each layer has unique attributes that affect operations. Cyberspace operations generally traverse all three layers of cyberspace but may target effects at one or more specific layers. Planners must consider the challenges and opportunities presented by each layer of cyberspace as well as the interactions amongst the layers. Figure 1-2 on page 1-6 depicts the relationship between the three cyberspace layers. The three cyberspace layers are—

- The physical network layer.
- The logical network layer.
- The cyber-persona layer.

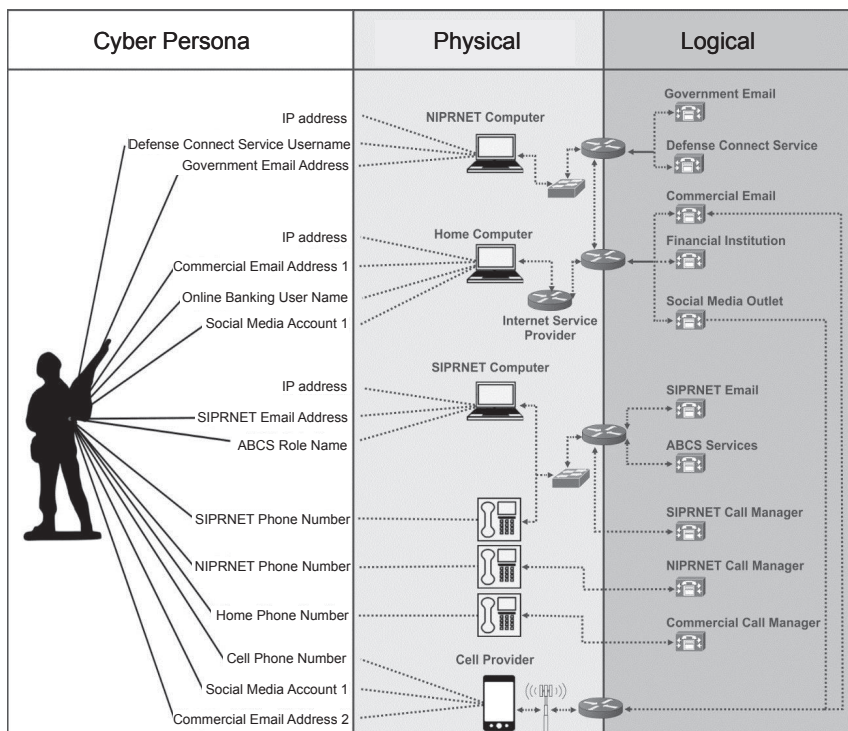
*See pp. 1-2 to 1-3 for related discussion from JP 3-12.*

### Physical Network Layer

The physical network layer consists of the information technology devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components (JP 3-12). Physical network components include the hardware and infrastructure such as computing devices, storage devices, network devices, and wired and wireless links. Components of the physical network layer require physical security measures to protect them from damage or unauthorized access, which, if left vulnerable, could allow a threat to gain access to both systems and critical data.

Every physical component of cyberspace is owned by a public or private entity. The physical layer often crosses geo-political boundaries and is one of the reasons that cyberspace operations require multiple levels of joint and unified action partner coordination. Cyberspace planners use knowledge of the physical location of friendly, neutral, and adversary information technology systems and infrastructures to understand appropriate legal frameworks for cyberspace operations and to estimate impacts of those operations. Joint doctrine refers to portions of cyberspace, based on who owns or controls that space, as either blue, gray, or red cyberspace (refer to JP 3-12). This publication refers to these areas as friendly, neutral, or enemy cyberspace respectively.





Ref: FM 3-12 (Aug '21), fig. 1-2. Relationship between the cyberspace network layers.

## Logical Network Layer

The logical network layer consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not necessarily tied to a specific physical link or node, but to their ability to be addressed logically and exchange or process data) (JP 3-12). Nodes in the physical layer may logically relate to one another to form entities in cyberspace not tied to a specific node, path, or individual. Web sites hosted on servers in multiple physical locations where content can be accessed through a single uniform resource locator or web address provide an example. This may also include the logical programming to look for the best communications route, instead of the shortest physical route, to provide the information requested.

## Cyber-Persona Layer

The cyber-persona layer is a view of cyberspace created by abstracting data from the logical network layer using the rules that apply in the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace, known as a cyber-persona (JP 3-12). Cyber-personas are not confined to a single physical or logical location and may link to multiple physical and logical network layers. When planning and executing cyberspace operations, staffs should understand that one actor or entity (user) may have multiple cyber-personas, using multiple identifiers in cyberspace. These various identifiers can include different work and personal emails and different identities on different Web forums, chatrooms, and social network sites. For example, an individual's account on a social media website, consisting of the username and digital information associated with that username, may be just one of that individual's cyber-personas.

# C. Operational & Mission Variables

Ref: Adapted from FM 3-12, *Cyberspace & Electronic Warfare Operations* (Apr '17), pp. 1-18 to 1-19.

Commanders and staffs use the operational and mission variables to help build their situational understanding. They analyze and describe an operational environment in terms of eight interrelated operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). Upon receipt of a mission, commanders filter information categorized by the operational variables into relevant information with respect to the mission. They use the mission variables, in combination with the operational variables, to refine their understanding of the situation and to visualize, describe, and direct operations. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).

*See pp. 4-2 to 4-8 for related discussion of the military decisionmaking process (MDMP) as related to cyberspace and electronic warfare operations.*

## Cyberspace and the Operational Variables (PMESII-PT)

Commanders and staffs continually analyze and describe the operational environment in terms of eight interrelated operational variables: political, military, economic, social, information, infrastructure, physical environment, and time. Each variable applied to an analysis of designated cyberspace can enable a more comprehensive understanding of the operational environment. The analysis describes the planning, preparation, execution, and assessment activities for both the wired and EMS portions cyberspace operations. The following are operational variable example questions specific to networks and nodes—

### P - Political

What networks and nodes require the most emphasis on security and defense to enable the functioning of the government?

### M - Military

Where are networks and nodes utilized by enemy and adversary actors to enable their activities?

### E - Economic

What networks and nodes require the most emphasis on security and defense to enable commerce and other economic-related activities?

### S - Social

What network nodes enable communication with the host nation population for the purpose of providing information or protecting them from potential negative effects caused by military operations in cyberspace?

### I - Information

What is the nature of the data transiting cyberspace that influences or otherwise affects military operations?

### I - Infrastructure

What networks and nodes enable critical infrastructure and key resource capabilities and supporting supervisory control and data acquisition systems?

## P - Physical Environment

How are wireless networks affected by the electromagnetic environment which includes terrain and weather?

## T - Time

What are the optimal times to create effects to support the overarching mission?

# Cyberspace and the Mission Variables (METT-TC)

The analysis of mission variables specific to cyberspace operations enables Army forces to integrate and synchronize cyberspace capabilities to support Army operations. Mission variables describe characteristics of the area of operations. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, and civil considerations. For cyberspace operations, mission variables provide an integrating framework upon which critical questions can be asked and answered throughout the operations process. The questions may be specific to either the wired portion of cyberspace, the EMS, or both. The following is a list of the mission variables example questions—

## M - Mission

Where can we integrate elements of cyberspace operations to support the unit mission? What essential tasks could be addressed by the creation of one or more effects by cyberspace operations?

## E - Enemy

How can we leverage information collection efforts regarding threat intentions, capabilities, composition, and disposition in cyberspace? What enemy vulnerabilities can be exploited by cyberspace capabilities?

## T - Terrain and Weather

What are the opportunities and risks associated with the employment of cyberspace operations capabilities when terrain and weather may cause adverse impacts on supporting information technology infrastructures?

## T - Troops and Support Available

What resources are available (internal and external) to integrate, synchronize, and execute cyberspace operations? What is the process to request, receive, and integrate these resources?

## T - Time Available

How can we synchronize OCO and related desired effects with the scheme of maneuver within the time available for planning and execution?

## C - Civil Considerations

How can we employ cyberspace operations without negative impacts on noncombatants?



*Refer to BSS6: The Battle Staff SMARTbook, 6th Ed. for further discussion. BSS6 covers the operations process (ADP 5-0); commander's activities; Army planning methodologies; the military decisionmaking process and troop leading procedures (FM 7-0 w/Chg 2); integrating processes (IPB, information collection, targeting, risk management, and knowledge management); plans and orders; mission command, C2 warfighting function tasks, command posts, liaison (ADP 6-0); rehearsals & after action reviews; and operational terms and military symbols (ADP 1-02).*

## II. Trends and Characteristics

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 1-8 to 1-12.

The rapid proliferation of cyberspace and EMS capabilities has further congested an already challenging OE. In addition to competing with threat actors in cyberspace and the EMS, U.S. forces also encounter challenges resulting from neutral actors. Such neutral systems as commercial aircraft and airports, Worldwide Interoperability for Microwave Access, and commercial cellular infrastructures contribute to continuing congestion in cyberspace and the EMS.

Several key trends and characteristics impact a commander's ability to use cyberspace and the EMS. Such trends and characteristics include—

- Congested environments.
- Contested environments.
- Threats.
- Hazards.
- Terrain.

### A. Congested Environments

Both cyberspace and the EMS are increasingly congested environments that friendly, neutral, and threat actors use to transmit and process large amounts of information. Since 2000, the Army's use of networked information systems in almost every aspect of operations has increased tenfold. Neutral and threat actors have similarly expanded their use of cyberspace and the EMS for a wide range of military and non-military purposes.

### B. Contested Environments

As cyberspace and the EMS continue to become more congested, the capabilities of state and non-state actors to contest U.S. advantages in both areas have also expanded. State and non-state threats use a wide range of advanced technologies that may represent relatively inexpensive ways for a small or materially disadvantaged adversary to pose a significant threat to the United States. The application of low-cost cyberspace capabilities can provide an advantage against a technology-dependent nation or organization and an asymmetric advantage to those who could not otherwise effectively oppose U.S. military forces.

### C. Threats

For every operation, threats are a fundamental part of an OE. 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). Threat is an umbrella term that includes any actor with the potential to harm the United States or its interests. Threats include—

- **Enemy.** An enemy is a party identified as hostile against which the use of force is authorized (ADP 3-0). An enemy is also called a combatant and treated as such under the laws of war. Enemies will employ various advanced technologies to attack Army forces in cyberspace and EMS to disrupt or destroy the ability to conduct operations or collect information that will give friendly forces a strategic, operational, or tactical advantage.
- **Adversary.** 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). Though an adversary is not treated as a combatant, the goal is still to prevent and deter conflict by keeping their activities within a desired state of cooperation and competition.
- **Peer Threat.** A peer threat is an adversary or enemy able to effectively oppose U.S. forces world-wide while enjoying a position of relative advantage in a specific region

(ADP 3-0), including cyberspace and the EMS. Peer threats often have cyberspace and EW capabilities that are comparable to U.S. capabilities. Peer threats may employ these capabilities across the competition continuum to collect intelligence, delay the deployment of U.S. forces, degrade U.S. capabilities, and disrupt U.S. operations. Peer threats have electromagnetic attack (EA) capabilities such as telecommunications and EMS jamming equivalent to or better than U.S. forces. Peer threats can conduct advanced cyberspace attacks, including denial-of-service, various forms of phishing, eavesdropping, and malware.

- **Hybrid Threat.** A hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, or criminal elements unified to achieve mutually benefitting effects (ADP 3-0). Commanders and staffs must understand that the diversity of a hybrid threat complicates operations since hostility is coming from multiple actors operating from various geographical territories. A hybrid threat complicates the United States' efforts to identify, characterize, attribute, and respond to threats in cyberspace and the EMS.
- **Organized Crime or other Non-State, Illegitimate Organizations.** These organizations often make sophisticated malware available for purchase or free, allowing even unsophisticated threat actors to acquire advanced capabilities at little to no cost. Because of the low barriers to entry and the potentially high payoff, the United States can expect an increasing number of adversaries to use cyberspace capabilities to attempt to negate U.S. advantages in military capability.
- **Insider Threat.** An insider threat is a person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of United States military forces (AR 381-12). Insider threats may include spies within or working with U.S. forces, as well as personnel who may be unaware of their actions either through deception or third party manipulation. Insider threats present unique challenges because they are trusted individuals with authorized access to Army capabilities and sensitive operational information. Insider threats may include spies within or working with U.S. forces.

*Note. Law enforcement and counterintelligence capabilities also operate in cyberspace during their efforts to neutralize criminal activities. Countering insider threats falls primarily within the purview of these organizations and outside the authorized activities of the cyberspace forces. However, information discovered in the course of authorized cyberspace operations may aid these other organizations.*

## D. Hazards

A hazard is a condition with the potential to cause injury, illness, or death of personnel, damage to or loss of equipment or property, or mission degradation (JP 3-33). Disruption to cyberspace's physical infrastructure often occurs due to operator errors, industrial accidents, and natural disasters. These unpredictable events may have just as significant impact on operations as the actions of enemies. Recovery from accidents and hazardous incidents may require significant coordination external to the DOD or the temporary reliance on backup systems with which operators may be less familiar.

Electromagnetic energy can also impact the operational capability of military forces, equipment, systems, and platforms. Various hazards from electromagnetic energy include electromagnetic environmental effects, electromagnetic compatibility issues, EMI, electromagnetic pulse, and electromagnetic radiation hazards.

Electromagnetic radiation hazards include hazards of electromagnetic radiation to personnel; hazards of electromagnetic radiation to ordnance; hazards of electromagnetic radiation to fuels; and natural phenomena effects such as space weather, lightning, and precipitation static.

# III. Core Competencies & Fundamentals

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 1-3 to 1-4.

## A. Core Competencies

Cyberspace forces and EW professionals are organized, trained, and equipped to provide the following core competencies that deliver essential and enduring capabilities to the Army—

- Enable situational understanding.
- Protect friendly personnel and capabilities.
- Deliver effects.

### Create Understanding

Cyberspace forces execute cyberspace intelligence, surveillance, and reconnaissance in and through the information environment to identify and understand adversary networks, systems, and processes. This information enables commanders to understand adversary capabilities and vulnerabilities, thereby enhancing the commanders' ability to prioritize and deliver effects.

EW professionals surveil the EMS to collect combat information used to characterize adversary use of the EMS and understand the integration of adversary emitter systems arrays at echelon. This information enables understanding friendly vulnerabilities and threat capabilities while allowing commanders to prioritize and deliver effects.

### Protect Friendly Personnel and Capabilities

Cyberspace forces defend networks, warfighting platforms, capabilities, and data from ongoing or imminent malicious cyberspace activity. By protecting critical networks and systems, cyberspace forces help maintain the Army's ability to conduct operations and project power across all domains.

EW forces, in coordination with the G-6 or S-6 and in support of the commander's directive, implement and enhance measures to protect friendly personnel, facilities, warfighting platforms, capabilities, and equipment from adverse effects in the EMS. EW forces recommend measures to mask or control friendly emissions from enemy detection and deny adversaries the ability to locate and target friendly formations. EW forces detect and mitigate enemy attacks in or through the EMS to maintain the Army's ability to conduct operations and project power across all domains.

### Deliver Effects

Cyberspace forces deliver cyberspace effects against adversary networks, systems, and weapons. These effects enhance the Army's ability to conduct operations, reduce adversary combat power, and project power across all domains.

EW professionals deliver effects in the EMS against adversary networks, systems, and weapons. These actions reduce adversary combat power, protect friendly forces, and enhance friendly forces and weapons' lethality.

## B. Fundamental Principles

Fundamental principles are basic rules or assumptions of central importance that guide how cyberspace and EW professionals' approach and conduct cyberspace operations and EW. These fundamental principles are—

- Operational focus.
- Adaptability and versatility.
- Global reach.



## Operational Focus

Cyberspace and EW forces execute missions in support of a commander's overarching operational design. When properly integrated and synchronized as part of a combined arms approach, cyberspace and EW capabilities can produce layered dilemmas for the adversary in multiple domains and enhance relative combat power. To accomplish this, cyberspace and EW staff must collaborate across all warfighting functions.

## Adaptability and Versatility

Cyberspace and EW forces conduct operations using capabilities that are adaptable to a variety of mission requirements. Cyberspace and EW capabilities vary in both the size of the force employed and the magnitude or scope of effects created. Depending on mission requirements, cyberspace and EW capabilities may be used as primary or supporting efforts for decisive, shaping or sustaining operations.

## Global Reach

The nature of the cyberspace domain increases the operational reach of cyberspace and EW forces. Combat mission force(s) and EW professionals deliver strategic, operational, or tactical effects worldwide from remote, co-located, or forward operating positions.

An operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Conditions in cyberspace and the EMS often change rapidly and can positively or negatively impact a commander's ability to achieve mission objectives. Friendly, neutral, adversary, and enemy actions in cyberspace and the EMS can create near-instantaneous effects on the battlefield or in garrison. Given the global nature of cyberspace and the EMS, these actions can impact a commander's OE even though the actions may originate or terminate beyond that OE. Cyberspace and EW effects also cross through and impact multiple domains simultaneously. For these reasons, commanders must gain and maintain an in-depth understanding of the OE that extends beyond the land domain to the multi-domain extended battlefield to seize, exploit, and retain operational initiative.

Operational initiative is the setting of tempo and terms of action throughout an operation (ADP 3-0). By gaining and maintaining positions of relative advantage, including information advantage in and through cyberspace and the EMS, commanders can seize and retain the operational initiative. To gain and maintain information advantage, commanders must account for the temporal nature of information and the temporary nature of many cyberspace and EW effects. On average, the relative operational advantage that a commander can gain from a piece of information or from a cyberspace or EW effect degrades over time. This means that a commander who takes action first, on average, will obtain a greater information advantage from a similar piece of information or effect than a commander who acts later. In this way, the commander who can sense, understand, decide, act, and assess faster than an opponent will generally obtain the greatest information advantage.

Commanders can use cyberspace and EW capabilities to gain enhanced situational awareness and understanding of the enemy through reconnaissance and sensing activities. These reconnaissance and sensing activities can augment and enhance the understanding a commander gains from information collection and intelligence processes. Commanders can also use cyberspace and EW capabilities to decide and act faster than an adversary or enemy. By protecting friendly information systems and signals from disruption or exploitation by an adversary or enemy, a commander can ensure command and control and maintain tactical and operational surprise. Conversely, a commander might use cyberspace and EW capabilities to slow or degrade an enemy's decision-making processes by disrupting enemy sensors, communications, or data processing. To make effective use of cyberspace and EW capabilities to achieve an information advantage, a commander must plan early to integrate cyberspace operations and EW actions fully into the overall scheme of maneuver.

## IV. Contributions to the Warfighting Functions

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 1-12 to 1-15.

This section describes how cyberspace operations and EW support the warfighting functions. It specifies the types of cyberspace operations and EW missions and actions that contribute to the various tasks related to each warfighting function.

### Command and Control

Commanders rely heavily on cyberspace and the EMS for command and control. At corps and below, the network in the command-and-control system is the Department of Defense information network-Army (DODIN-A). The Department of Defense information network-Army is an Army-operated enclave of the DODIN that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide (ATP 6-02.71). Signal forces establish, manage, secure, and defend the DODIN-A by conducting Department of Defense information network operations and maintaining cybersecurity compliance to prevent intrusions into the DODIN-A. EW supports command and control through electromagnetic protection (EP) to eliminate or mitigate the negative impact of friendly, neutral, enemy, or naturally occurring EMI on command-and-control systems. The frequency assignment and deconfliction tasks of spectrum management operations support EP. Such EP tasks include—emission control, mitigating electromagnetic environmental effects, electromagnetic compatibility, electromagnetic masking, preemptive countermeasures, and electromagnetic warfare reprogramming. These tasks require integration with spectrum management operation for frequency management and deconfliction.

### Movement and Maneuver

Cyberspace operations and EW enhance friendly forces commanders' movement and maneuver by disrupting adversary command and control, reducing adversary and increasing friendly situational awareness, and negatively affect the adversary's ability to make sound decisions. Due to the range and reach of cyberspace capabilities, cyberspace forces are often able to support friendly maneuver in close areas while simultaneously supporting deep area operations.

DODIN operations support movement and maneuver by establishing secure tactical networks that allow communications with friendly forces conducting operations laterally in close and deep areas, in addition to communications with higher headquarters in the rear area. Units use the DODIN-A as the primary means of communication during movement and maneuver. Satellite communications, combat net radios, and wired networks are elements of the DODIN-A used to synchronize operations, collaborate, understand the environment, and coordinate fires. The network enables near real-time updates to the common operational picture. The upper and lower tiers of the DODIN-A connect headquarters to subordinate, adjacent, and higher headquarters and unified action partners.

Offensive cyberspace operations (OCO) in coordination with other forms of fires also support movement and maneuver by opening avenues necessary to disperse and displace enemy forces. Synchronizing OCO with other fires sets conditions that enable maneuver to gain or exploit positions of relative advantage.

EW assets support movement and maneuver by conducting operations to degrade, neutralize, or destroy enemy combat capabilities in the EMS. Defensive EA protects friendly forces from enemy attacks during movement and maneuver by denying the enemy the use of the EMS. Using friendly EA to counter radio-controlled devices, such as improvised explosive devices, drones, robots, or radio-guided munitions is an example of defensive EA. During defensive EA, EW assets conduct operations to degrade, neutralize, or destroy enemy combat capabilities in the EMS. EW assets conduct defensive EA by employing EA capabilities such as counter radio-controlled improvised explosive device electronic warfare and devices used for aircraft survivability. Offensive EA supports

movement and maneuver by projecting power within the time and tempo of the scheme of maneuver. Electromagnetic jamming, electromagnetic intrusion, and electromagnetic probing are examples of offensive EA. Electromagnetic support (ES) supports movement and maneuver by providing combat information for a situational understanding of the OE.

## Intelligence

Cyberspace operations, EW, and intelligence mutually identify the cyberspace and EMS aspects of the OE to provide recommendations for friendly courses of action during the military decision-making process. Cyberspace and EW forces support information collection that may be used by intelligence professionals. Conversely, intelligence operations provide products that enhance understanding of the OE, enable targeting, and support defense in cyberspace and the EMS. It is critical that information acquired through cyberspace operations and EW is standardized and reported to the intelligence community. Intelligence supports cyberspace operations through the intelligence process, intelligence preparation of the battlefield (IPB), and information collection. Intelligence at all echelons supports cyberspace operations and EW planning, and helps measure performance and effectiveness through battle damage assessment. Cyberspace planners leverage intelligence analysis, reporting, and production capabilities to understand the OE, develop plans and targets, and support operations throughout the operations process. In the context of cyberspace and the EMS, the OE includes network topology overlays that graphically depict how information flows and resides within the operational area and how the network transports data in and out of the area of interest.

## Fires

OCO and EA tasks are part of the fires warfighting function. Cyberspace forces employ cyberspace attacks to deny, degrade, disrupt, and destroy or otherwise affect enemies' cyberspace or information-dependent capabilities. EW personnel employ EA to degrade, and neutralize the enemies' ability to use the EMS. Cyberspace and EW effects transcend beyond cyberspace and the EMS and may result in second-and-third-order effects that could impact the other physical domains. Army cyberspace and EW effects applied against enemy capabilities and weapon systems deny their ability to communicate, track, or target. EW also supports fires by enabling lethal fires through the employment of ES to search for, identify, and locate or localize sources of radiated electromagnetic energy used by the enemy for targeting. Defensive EA can support fires through the deployment of decoys or noise to mask friendly fires networks.

## Sustainment

Cyberspace operations support sustainment through DODIN operations and defensive cyberspace operations (DCO). Sustainment organizations, functions, systems, and sustainment locations are highly dependent on DODIN operations. DODIN operations establish the necessary communications to conduct sustainment functions. Cyberspace forces defend sustainment systems when adversaries breach cybersecurity measures of networks and systems from threat cyberspace attacks. EW supports sustainment through EP and ES, ensuring freedom of action for DODIN operations in and through the EMS for continued sustainment support. Management, coordination, and deconfliction of frequencies in the EMS are functions of spectrum management operations.

## Protection

DCO-IDM and EP tasks, in addition to the cyberspace security tasks of DODIN operations, are part of the protection warfighting function. DODIN operations, DCO-IDM, EP, and defensive EA support protection by securing and defending the DODIN-A. Cyberspace forces conduct DCO-IDM to detect, characterize, counter, and mitigate ongoing or imminent threats to the DODIN-A. DODIN operations and DCO-IDM also enable other protection tasks by providing secured communications for area security, police operations, personnel recovery, air and missile defense, and detention operations. EP involves actions to protect personnel, facilities, and equipment from friendly, neutral, or enemy use of the EMS. EP includes measures to protect friendly personnel and equipment in a contested and congested electromagnetic operational environment (EMOE).

Adversaries continue to develop sophisticated weapons and networked systems that project power through or depend on cyberspace and the EMS. The Army employs cyberspace and EW capabilities as part of a joint and combined arms approach to defeat threat activities in cyberspace and the EMS, protect friendly forces, and enable friendly freedom of action across the conflict continuum. Army cyberspace and EW forces apply the following core competencies and underlying fundamental principles to ensure friendly forces gain and maintain positions of relative advantage.

## V. Conflict and Competition

Army forces face continuous competition and conflict in cyberspace and the EMS from threats intending to diminish friendly capabilities. Commanders must seek and exploit opportunities for success in cyberspace and the EMS wherever and whenever authorized.

### A. Competition Continuum

Cyberspace operations, EW, and spectrum management operations take place across the competition continuum. The competition continuum describes a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict. Superiority in cyberspace and the EMS enables U.S. forces to conduct operations to achieve the goals and accomplish the objectives assigned to them by the President and Secretary of Defense. Though U.S. forces may conduct cyberspace operations and EW during competition below the level of armed conflict, they are critical enablers to combat power when conducting large-scale combat operations during armed conflict. Competition below armed conflict consists of situations in which joint forces take actions outside of armed conflict against a strategic actor in pursuit of policy objectives.

Spectrum management operations fulfill a crucial within the CEMA construct. Spectrum management operations take place across the entire competition continuum and ensure proper coordination of EMS activities spanning the entirety of military operations.

### B. Multi-Domain Extended Battlefield

The enemy seeks to employ capabilities to create effects in multiple domains to counter U.S. interests and impede friendly operations. Threat actors will conduct activities in the information environment, space, and cyberspace to influence U.S. decision makers and disrupt the deployment of friendly forces. Land-based threats will attempt to impede joint force freedom of action across the air, land, maritime, space, and cyberspace domains. They will disrupt the EMS, sow confusion, and challenge the legitimacy of U.S. actions. Understanding how threats can present multiple dilemmas to Army forces in all domains helps Army commanders identify (or create), seize, and exploit their opportunities. Implementing operations security (OPSEC) is critical to protecting essential friendly information technology infrastructures, command and control, and targeting systems. Operations security is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities (JP 3-13.3).

*See also pp. 2-4 to 2-5.*

### C. Positions of Relative Advantage (in Cyberspace and the Electromagnetic Spectrum)

The Army conducts cyberspace operations and EW to attain positions of relative advantage in cyberspace and the EMS, to establish information superiority. 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 (ADP 3-0).

# II. Cyberspace Operations

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), chap. 2.

**Cyberspace operations and electromagnetic warfare (EW)** can benefit from synchronization with other Army capabilities using a combined arms approach to achieve objectives against enemy forces. Cyberspace operations and EW can provide commanders with positions of relative advantage in the multi-domain fight. Effects that bleed over from the cyberspace domain into the physical domain can be generated and leveraged against the adversary. A cyberspace capability is a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace (JP 3-12).

## Electromagnetic Spectrum Superiority

Electromagnetic spectrum superiority is the degree of control in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting the threat's ability to do the same (JP 3-85). Electromagnetic warfare (EW) creates effects in the EMS and enables commanders to gain EMS superiority while conducting Army operations. EW capabilities consist of the systems and weapons used to conduct EW missions to create lethal and non-lethal effects in and through the EMS.

See chap. 3, *Electromagnetic Warfare (EW)*, for further discussion.

## I. Cyberspace Operations

The joint force and the Army divide cyberspace operations into three categories based on the portion of cyberspace in which the operations take place and the type of cyberspace forces that conduct those operations. Each of type of cyberspace operation has varying associated authorities, approval levels, and coordination considerations. An Army taxonomy of cyberspace operations is depicted in figure 2-1, below. The three types of cyberspace operations are—

### Cyberspace Operations



**DODIN Operations**



**Defensive Cyberspace Operations (DCO)**



**Offensive Cyberspace Operations (OCO)**

The Army conducts DODIN operations on internal Army and DOD networks and systems using primarily signal forces. The Army employs cyberspace forces to conduct DCO which includes two further sub-divisions—DCO-IDM and defensive cyberspace operations-response actions (DCO-RA). Cyberspace forces conduct DCO-IDM within the DODIN boundary, or on other friendly networks when authorized, in order to defend those networks from imminent or ongoing attacks. At times cyberspace forces may also take action against threat cyberspace actors in neutral or adversary

networks in defense of the DODIN or friendly networks. These types of actions, called DCO-RA, require additional authorities and coordination measures. Lastly, cyberspace forces deliberately target threat capabilities in neutral, adversary, and enemy-held portions of cyberspace by conducting OCO. Cyberspace forces may include joint forces from the DOD cyber mission forces or Army-retained cyberspace forces.

*See pp. 2-27 to 2-36 for discussion of cyberspace forces.*

## A. Department of Defense Information Network Operations (DODIN)

The Department of Defense information network is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. Also called DODIN (JP 6-0). This includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Department of Defense information network operations are operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network. Also called DODIN operations (JP 3-12). DODIN operations provide authorized users at all echelons with secure, reliable end-to-end network and information system availability. DODIN operations allow commanders to effectively communicate, collaborate, share, manage, and disseminate information using information technology systems.

Signal forces install tactical networks, conduct maintenance and sustainment activities, and security evaluation and testing. Signal forces performing DODIN operations may also conduct limited DCO-IDM. Since both cyberspace security and defense tasks are ongoing, standing orders for DODIN operations and DCO-IDM cover most cyberspace security and initial cyberspace defense tasks.

The Army secures the DODIN-A using a layered defense approach. Layered defense uses multiple physical, policy, and technical controls in to guard against threats on the network. Layering integrates people, technology, and operational capabilities to establish security barriers across multiple layers of the DODIN-

A. Various types of security barriers include—

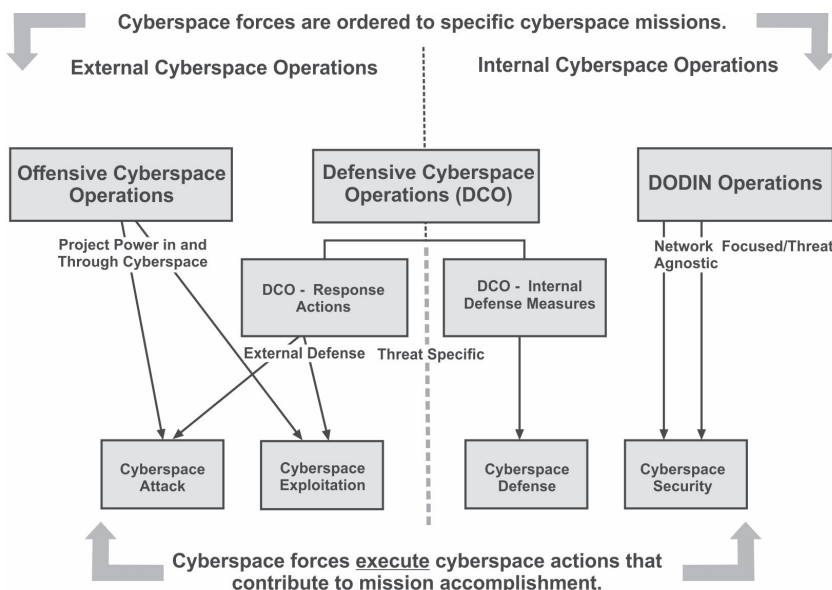
- Antivirus software.
- Firewalls.
- Anti-spam software.
- Communications security.
- Data encryption.
- Password protection.
- Physical and technical barriers.
- Continuous security training.
- Continuous network monitoring.

Security barriers are protective measures against acts that may impair the effectiveness of the network, and therefore the mission command system. Additionally, layering includes perimeter security, enclave security, host security, physical security, personnel security, and cybersecurity policies and standards. Layering protects the cyberspace domain at the physical, logical, and administrative control levels.

## B. Defensive Cyberspace Operations (DCO)

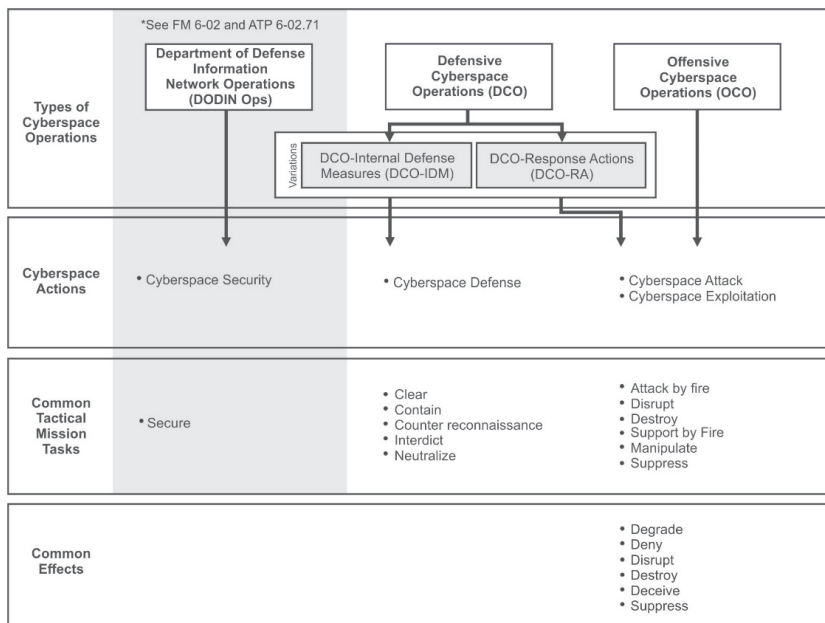
Defensive cyberspace operations are missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices,

# Cyberspace Operations (Missions & Actions)



Cyberspace Operations

Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), fig. 2-2. Cyberspace operations missions and actions.



Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), fig. 2-1. Cyberspace operations taxonomy.



and other designated systems by defeating on-going or imminent malicious cyberspace activity (JP 3-12). The term blue cyberspace denotes areas in cyberspace protected by the United States, its mission partners, and other areas the Department of Defense may be ordered to protect. DCO are further categorized based on the location of the actions in cyberspace as—

## **Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM)**

Defensive cyberspace operations-internal defensive measures are operations in which authorized defense actions occur within the defended portion of cyberspace (JP 3-12). DCO-IDM is conducted within friendly cyberspace. DCO-IDM involves actions to locate and eliminate cyber threats within friendly networks. Cyberspace forces employ defensive measures to neutralize and eliminate threats, allowing reestablishment of degraded, compromised, or threatened portions of the DODIN. Cyberspace forces conducting DCO-IDM primarily conduct cyberspace defense tasks, but may also perform some tasks similar to cyberspace security.

Cyberspace defense includes actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include 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. (JP 3-12). Cyberspace forces act on cues from cybersecur-ity or intelligence alerts of adversary activity within friendly networks. Cyberspace defense tasks during DCO-IDM include hunting for threats on friendly networks, deploying advanced countermeasures, and responding to eliminate these threats and mitigate their effects.

## **Defensive Cyberspace Operations-Response Actions (DCO-RA)**

Defensive cyberspace operation-response actions are operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without permission of the owner of the affected system (JP 3-12). DCO-RA take place outside the boundary of the DODIN. Some DCO-RA may include actions that rise to the level of use of force and may include physical damage or destruction of enemy systems. DCO-RA consist of conducting cyberspace attacks and cyberspace exploitation similar to OCO. However, DCO-RA use these actions for defensive purposes only, unlike OCO that is used to project power in and through cyberspace.

Decisions to conduct DCO-RA depend heavily on the 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 threat has or is expected to cause, and national policy considerations. DCO-RA are conducted by national mission team(s) and require a properly coordinated military order, coordination with interagency and unified action partners, and careful consideration of scope, rules of engagement, and operational objectives.

## **C. Offensive Cyberspace Operations (OCO)**

Offensive cyberspace operations are missions intended to project power in and through cyberspace (JP 3-12). Cyberspace forces conduct OCO outside of DOD networks to achieve positions of relative advantage through cyberspace exploitation and cyberspace attack actions in support of commanders' objectives. Commanders must integrate OCO within the combined arms scheme of maneuver throughout the operations process to achieve optimal effects.

The Army provides cyberspace forces trained to perform OCO across the range of military operations to the joint force. Army forces conducting OCO do so under the authority of a joint force commander. Refer to Appendix C for information on integrat-

ing with unified action partners. Joint forces may provide OCO support to corps and below Army commanders in response to requests through the joint targeting process. Refer to Appendix D for more information on joint cyberspace forces. Targets for cyberspace effects may require extended planning time, extended approval time, as well as synchronization and deconfliction with partners external to the DOD. Chapter 4 covers targeting considerations in detail.

## II. Cyberspace Actions

Execution of these cyberspace operations entails one or more specific tasks, which joint cyberspace doctrine refers to as cyberspace actions (refer to JP 3-12), and the employment of one or more cyberspace capabilities. Figure 2-2 on page 2-6 depicts the relationships between the types of cyberspace operations and their associated actions, the location of those operations in cyberspace, and the forces that conduct those operations. The four cyberspace actions are—

### A. Cyberspace Security

Cyberspace security is actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (JP 3-12). These preventive measures include protecting the information on the DODIN, ensuring the information's availability, integrity, authenticity, confidentiality, and nonrepudiation. Cyberspace security is generally preventative in nature, but also continues throughout DCO-IDM and incident responses in instances where a cyberspace threat compromises the DODIN. Some common types of cyberspace security actions include—

- Password management.
- Software patching.
- Encryption of storage devices.
- Mandatory cybersecurity training for all users.
- Restricting access to suspicious websites.
- Implementing procedures to define the roles, responsibilities, policies, and administrative functions for managing DODIN operations.

### B. Cyberspace Defense

Cyberspace defense are actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include 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. (JP 3-12)

### C. Cyberspace Exploitation

Cyberspace exploitation consists of actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations (JP 3-12). These operations must be authorized through mission orders and are part of OCO or DCO-RA actions in gray or red cyberspace that do not create cyberspace attack effects, and are often intended to remain clandestine. Cyberspace exploitation includes activities to support operational preparation of the environment for current and future operations by gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage within cyberspace; and positioning cyberspace capabilities to facilitate follow-on actions. Cyberspace exploitation actions are deconflicted with other United States Government departments and agencies in accordance with national policy.

# D. Cyberspace Attack

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), p. 2-7.

Cyberspace attack actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains (JP 3-12). A cyberspace attack creates effects in and through cyberspace and may result in physical destruction. Modification or destruction of cyberspace capabilities that control physical processes can lead to effects in the physical domains. Some illustrative examples of common effects created by a cyberspace attack include—

## Deny

To prevent access to, operation of, or availability of a target function by a specified level for a specified time (JP 3-12). Cyberspace attacks deny the enemy's ability to access cyberspace by hindering hardware and software functionalities for a specific duration of time.

## Degrade

To deny access to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation is specified. If a specific time is required, it can be specified (JP 3-12).

## Disrupt

To completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent (JP 3-12). Commanders can use cyberspace attacks that temporarily but completely deny an enemy's ability to access cyberspace or communication links to disrupt decision making, ability to organize formations, and conduct command and control. Disruption effects in cyberspace are usually limited in duration.

## Destroy

To completely and irreparably deny access to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted (JP 3-12). Commanders can use cyberspace attacks to destroy hardware and software beyond repair where replacement is required to restore system function. Destruction of enemy cyberspace capabilities could include irreversible corruption to system software causing loss of data and information, or irreparable damage to hardware such as the computer processor, hard drive, or power supply on a system or systems on the enemy's network.

## Manipulate

Manipulation, as a form of cyberspace attack, controls or changes information, information systems, and/or networks in gray or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. It uses an adversary's information resources for friendly purposes, to create denial effects not immediately apparent in cyberspace (JP 3-12). Commanders can use cyberspace attacks to manipulate enemy information or information systems in support of tactical deception objectives or as part of joint military deception. Refer to FM 3-13.4 for information on Army support to military deception.

*Note. Cyberspace attacks are types of fires conducted during DCO-RA and OCO actions and are limited to cyber mission force(s) engagement. They require coordination with other United States Government departments and agencies and careful synchronization with other lethal and non-lethal effects through established targeting processes.*

### III. Interrelationship with Other Operations

This section describes the relationship that cyberspace operations and EW have with other operations. It discusses how cyberspace operations and EW mutually support intelligence operations, space operations, and information operations.

#### A. Intelligence Operations

As an operation, intelligence is (1) the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations; (2) the activities that result in the production; and (3) the organizations engaged in such activities (JP 2-0). Intelligence at all echelons supports the planning of cyberspace operations and EW and assists with defining measures of performance and effectiveness. Intelligence also assists the fires support element in developing the high payoff target (HPT) list, and collaborating with the CEMA section to ensure the high payoff target list includes enemy cyberspace and EW-related targets. Intelligence also plays a crucial part in assisting the fires support element in continued target development, including forwarding targets to the joint task force (JTF) headquarters for assessment as potential targets for the joint targeting list.

Information collection supports cyberspace operations and EW by collecting information to satisfy commander's critical information requirement(s) (CCIRs) and staff members' information requirements (IRs) regarding friendly, neutral, and enemy cyberspace and EMS capabilities, activities, disposition, and characteristics within the OE. Information collection also drives capability development. A robust intelligence package is imperative to understanding the target space, developing tools and having meaningful effects in cyberspace. There are four tasks and missions nested in information collection: intelligence operations, reconnaissance, surveillance, and security operations (See Chapter 4).

Information obtained by information collection drives the IPB process. Through the IPB process, the G-2 or S-2 analyzes operational and mission variables in an area of interest to determine their effect on operations. These variables affect how friendly forces will conduct cyberspace operations and EW within the assigned AO. Conversely, cyberspace operations and EW also contribute to intelligence by supporting information collection. Cyberspace operations and EW capabilities collect combat information to answer CCIRs and IRs for situational awareness and targeting.

SIGINT, cyberspace operations, and EW may overlap during operations in the EMS. For this reason, effective integration of SIGINT, cyberspace, EW, and spectrum management operations extends well beyond simple coordination. Effective integration requires both deconfliction and identification of windows of opportunity among these operations. This integration requires close staff collaboration, detailed procedural controls, and various technical channels. See Chapter 4 for additional details.

The intelligence staff also identifies adversary and enemy key terrain as part of the IPB process. Cyberspace operations use the concept of key terrain as a model to identify critical aspects of the cyberspace domain. Identified key terrain in cyberspace is subject to actions the controlling combatant (friendly, enemy, or adversary) deems advantageous such as defending, exploiting, and 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 that require priorities for defense.
- Locations in cyberspace that friendly forces require access for essential functions or capabilities.

## B. Space Operations

Cyberspace and space operations are interdependent. Access to the space domain is critical to cyberspace operations, especially DODIN operations, enabling global end-to-end network connectivity. In the Army, the space domain is only accessible through space operations. Conversely, space capabilities such as navigation warfare, offensive space control, and defensive space control are dependent on operations conducted in space, cyberspace, and the EMS. This interrelationship is critical, and addressing the interdependencies between the three must be managed throughout the operations process.

Both cyberspace operations and EW can affect space operations. Ground control systems that control satellites rely on networked computers to maintain orbital parameters and direct onboard sensors, particularly to maintain stable orbits; radios transmit computer commands to the satellites. Computer code sent directly to satellites in orbit can potentially allow remote control of the system, preventing others' access to onboard sensors or communications systems. Adversaries could similarly enter ground control systems and issue alternative orders to satellites to move them out of position or shut off critical systems. Because satellites routinely receive commands using radio frequencies, an adversary might attempt to shut off sensors or directly gain control of the spacecraft, rather than trying to issue orders through a ground control system.

All space operations rely on the EMS for command and control, sensing, and information distribution. The vital nature of space operations in multi-domain operations requires close coordination with other EMS activities associated with spectrum management operations to ensure proper prioritization, integration, synchronization, and deconfliction. The G-2 or S-2 uses information gathered through space-based intelligence, surveillance, and reconnaissance to assist the commander and staff with attaining situational awareness and understanding of the OE.

Navigation warfare is the deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electromagnetic warfare operations (JP 3-14). A navigation warfare attack denies threat actors a global navigation satellite system through various methods, including OCO, space operations, and EA. Global navigation satellite system is the general term used to describe any space-based system providing positioning, navigation, and timing (PNT) information worldwide (for example, Global Positioning System). Navigation warfare effectiveness requires synchronization of space operations, cyberspace operations, and EW capabilities with lethal and nonlethal attack actions to create desired effects. EW must be synchronized with space operations to understand the impacts of navigation warfare operations, deny adversary access to global navigation satellite system information, and protect friendly spectrum-dependent devices using specific frequencies within the EMS.

*Refer to FM 3-14 for more information on navigation warfare.*

The space domain consists of three segments: space, link, and ground. The space segment is the operational area corresponding with the space domain and comprises satellites in both geosynchronous and non-geosynchronous Earth orbit. The link segment consists of signals connecting ground and space segments through the EMS. The ground segment consists of ground-based facilities and equipment supporting command and control of space assets, ground-based processing equipment, earth terminals, user equipment, space situational awareness sensors, and the interconnectivity between the facilities and equipment. Earth terminals include all multi-Service ground, shipborne, submarine, and airborne satellite terminals that establish connectivity to the satellites in the space segment. The three space domain segments rely heavily on cyberspace operations to protect networking and information technologies and infrastructures while depending on the EMS to conduct operations between the space, link, and ground segments.

Cyberspace operations contribute to space operations by protecting friendly networks that leverage the global navigation satellite system while targeting similar enemy and adversary capabilities. Additionally, cyberspace operations establish network connectivity between ground-based facilities and equipment throughout the space domain's ground segment. EW supports navigation warfare by denying the enemy access to global navigation satellite system information while protecting friendly space capabilities operating in the EMS.

Integrating cyberspace operations, EW, and space operations enable commanders and staffs at each level to synchronize capabilities and effects. Space-based capabilities (space segment) enable distributed and global cyberspace operations. Cyberspace and space-based capabilities provide responsive and timely support that allows commanders to project combat power from the highest echelons down to the tactical level. Synchronization with spectrum management operations is necessary to ensure the availability of resources in the EMS and to prevent spectrum conflicts.

*Refer to FM 3-14 for more information about space operations.*

## C. Information Operations (IO)

Information operations are the integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (JP 3-13). Information operations (IO) integrate and synchronize information-related capabilities to create effects in and through the information environment and deliver an operational advantage to the commander. IO optimize the information element of combat power and support and enhance all other elements to gain operational advantage over a threat. IO consist of three inter-related efforts that work in tandem and overlap each other. These three efforts are—

- A commander-led staff planning and synchronization effort.
- A preparation and execution effort carried out by information-related capabilities units, IO units, or staff entities in concert with the IO working group.
- An assessment effort that is carried out by all involved.

When commanders employ cyberspace and EW capabilities to create desirable conditions within the OE, they synchronize these actions through IO. Commanders use cyberspace operations and EW to gain a strategic advantage in cyberspace and the EMS. Cyberspace and EW capabilities support operations by enabling the ability to share information among friendly forces or affecting the enemy's ability to use cyberspace and the EMS.

Cyberspace operations and EW effects influence, disrupt, corrupt, or manipulate the decision-making cycle of threat actors. Cyberspace operations support operations through OCO or DCO-RA by creating denial or manipulation effects to degrade, disrupt, or destroy the enemy's cyberspace capability or change enemy information, information systems, or networks. EW supports operations through EA by degrading, neutralizing, or destroying enemy capability to use the EMS. EW also supports operations through EP actions by concealing or manipulating friendly EMS signatures, to degrade or deceive enemy sensors or targeting systems. When integrated and synchronized with other capabilities, cyberspace operations and EW can help commanders set favorable conditions for information advantage, whether in cyberspace, the EMS, or other domains.

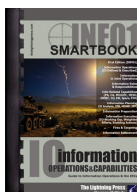
Cyberspace operations and EW can also create cognitive effects by impacting physical components of enemy capabilities. For example, affecting the ability of an enemy's fires network through a cyberspace attack or EA may deny or create doubt about their ability to use artillery effectively. Similarly, restricting the enemy's ability to use cyberspace or EMS at critical points can affect enemy judgments when exercising command and control. Synchronizing defensive EW and cyberspace operations

with other capabilities can also disrupt a threat's ability to make decisions while ensuring friendly forces freedom of action.

Cyberspace operations and EW synchronized through the operations process and targeting can provide commanders additional ways and means to—

- Affect threat capabilities that inform or influence decision making.
- Affect threat capabilities for command and control, movement and maneuver, fires, intelligence, communications, and information warfare.
- Affect threat capabilities to target and attack friendly command and control and related decision support systems.
- Affect threat capabilities that distribute, publish, or broadcast information designed to persuade relevant actors to oppose friendly operations.
- Enable military deception directed against threat decision making, intelligence and information gathering, communications, dissemination, and command and control capabilities.
- Enable friendly OPSEC to protect critical information.
- Enable friendly influence activities, such as military information support operations, to improve or sustain positive relations with foreign actors in and around the operational area and to degrade threat influence over the same.
- Protect friendly information, technical networks, and decision-making capabilities from exploitation by enemy and adversary information warfare assets.

See pp. 0-10 to 0-16 for further discussion of information operations.



Refer to INFO1: *The Information Operations & Capabilities SMARTbook (Guide to Information Operations & the IRCs)*. INFO1 chapters and topics include information operations (IO defined and described), information in joint operations (joint IO), information-related capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution (IO working group, IO weighted efforts and enabling activities, intel support), fires & targeting, and information assessment.



# III. Army Organizations & Command and Control

*Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), chap. 3.*

Army maneuver commanders use cyberspace operations and EW to understand the OE, support decision-making, and affect adversaries. Maneuver commanders at the brigade combat team level and above rely on assigned CEMA sections to leverage Army and joint cyberspace and EW capabilities. During joint operations, a corps or division designated as a JTF headquarters or a joint force headquarters combines its spectrum management chief with its CEMA section to establish an electromagnetic spectrum operations (EMSO) cell to support the joint electromagnetic spectrum operations cell (JEMSOC). Numerous Army and joint organizations contribute forces and capabilities for use in cyberspace operations and EW. Commanders at corps and below should possess a general understanding of the roles and responsibilities of these organizations and how they interact with the units' CEMA sections.

## I. United States Army Cyber Command

ARCYBER operates and defends Army networks and delivers cyberspace effects against adversaries to defend the nation. ARCYBER rapidly develops and deploys cyberspace capabilities to equip our force for the future fight against a resilient, adaptive adversary. ARCYBER also integrates intelligence, fires, space, psychological operations, strategic communications, public affairs, special technical operations, cyberspace operations, electromagnetic warfare, and information operations to allow Army commanders a decisional advantage during competition and conflict.

ARCYBER protects DODIN-A through DCO-IDM and DODIN operations. Commander, ARCYBER, is also the commander of joint force headquarters-cyber (JFHQ-C [Army]). In this role, Commander, ARCYBER, possesses the capability to conduct OCO to attack and exploit the enemy upon authorization from United States Cyber Command (USCYBERCOM). ARCYBER is the Army's point of contact for reporting and assessing cyber incidents and events involving suspected adversary activity. The United States Army Network Enterprise Technology Command (NETCOM) and the regional cyber center act as the chief action arms, having been delegated operational control and directive authority for cyberspace operations by ARCYBER for DODIN operations over all Army networks. ARCYBER serves as the Army's principal cybersecurity service provider and provides program oversight while NETCOM and the regional cyber centers act as the principal executors of the program. Units assigned to ARCYBER are—

- NETCOM.
- 1st Information Operations Command (Land).
- 780th Military Intelligence Brigade.
- Cyber protection brigade.
- 915th Cyber Warfare Battalion.

## II. Army Information Warfare Operations Center

The Army Information Warfare Operations Center serves as ARCYBER's hub for coordinating, integrating, synchronizing, and tracking cyberspace operations, electromagnetic warfare (EW), IO, and answering intelligence requirements in support

of national, regional, and Army directives. The Army Information Warfare Operations Center maintains global and regional situational awareness and understanding while executing mission command of all assigned or allocated Army cyber and IO forces.

The Army Information Warfare Operations Center is composed of personnel with information-related capabilities expertise (IO, cyber, EW, psychological operations [forces], public affairs, civil affairs, military deception, United States Space Command and special technical operations), to include representatives from all staff functions and embeds from partner organizations. The Army Information Warfare Operations Center is responsible for integrating information-related capabilities across the staff into the command's current operations and plans processes. Additionally, the Army Information Warfare Operations Center —

- Receives reports from subordinate commands.
- Prepares reports required by higher headquarters.
- Processes requests for support (RFS).
- Publishes operation orders (OPORDs) and cyber tasking orders (CTOs).
- Consolidates Commander's critical information requirements.
- Answers requests for information from higher HQs, CCMDs, other Services and agencies.
- Assesses the overall progress of ongoing operations.

### III. Cyberspace Electromagnetic Activities at Corps and Below

CEMA sections are assigned to the G-3 or S-3 within corps, divisions, BCTs, and combat aviation brigades. Commanders are responsible for ensuring that CEMA sections integrate cyberspace operations and EW into their concept of operations. The CEMA section involves key staff members in the CEMA working group to assist in planning, development, integration, and synchronization of cyberspace operations and EW.

*Note. The structure of the CEMA section is similar at all corps and below echelons. However, 1st IO Command may augment a corps' CEMA section to provide increased capabilities for synchronizing and integrating cyberspace operations and EW with IO.*

#### A. Commander's Role

Commanders direct the continuous integration of cyberspace operations and EW within the operations process, whether in a tactical environment or at home station. By leveraging cyberspace operations and EW as part of combined arms approach, commanders can sense, understand, decide, act, and assess faster than the adversary assesses and achieve a decisional advantage in multiple domains during operations.

Commanders should—

- Include cyberspace operations and EW within the operations process.
- Continually enforce cybersecurity standards and configuration management.
- Understand, anticipate, and account for cyberspace and EW effects, capabilities, constraints, and limitations, including second and third order effects.
- Understand the legal and operational authorities to affect threat portions of cyberspace or EMS.
- Understand the implications of cyberspace operations and EW operations on the mission and scheme of maneuver.
- Understand how the selected course of action (COA) affects the prioritization of

resources to their portion of the DODIN-A.

- Leverage effects in and through cyberspace and the EMS to support the concept of operations.
- Develop and provide intent and guidance for actions and effects inside and outside of the DODIN-A.
- Identify critical missions or tasks in phases to enable identification of key terrain in cyberspace.
- Ensure active collaboration across the staff, subordinate units, higher headquarters, and unified action partners that enable a shared understanding of cyberspace and the EMS.
- Approve high-priority target lists, target nominations, collection priorities, and risk mitigation measures.
- Ensure the synchronization of cyberspace operations and EW with other lethal and nonlethal fires to support the concept of operations.
- Oversee the development of cyberspace operations and EW-related home-station training.

## B. Cyberspace Electromagnetic Activities (CEMA) Section

The CEMA section plans, coordinates, and integrates OCO, DCO and EW in support of the commander's intent. The CEMA section collaborates with numerous staff sections to ensure unity of effort in meeting the commander's total operational objectives such as collaborating with the G-2 or S-2 to attain situation awareness and understanding of friendly, enemy, and neutral actors operating within the AO. The CEMA section is responsible for providing regular updates to the commander and staff on OCO and other supported operations conducted in the AO. The CEMA section is responsible for synchronizing and integrating cyberspace operations and EW with the operations process and through other integrating processes. Personnel assigned to the CEMA section are the—

- CEWO.
- Cyber warfare officer.
- EW technician.
- EW sergeant major (corps) or EW NCOIC (division).
- EW noncommissioned officer (NCO).
- CEMA spectrum manager.

*See following pages (pp. 2-30 to 2-31) for an overview and further discussion.*

## C. Cyberspace Electromagnetic Activities (CEMA) Working Group

The CEMA section leads 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 CEWO uses a CEMA working group to assist in synchronizing and integrating cyberspace operations and EW 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 will vary based on mission requirements.

If scheduled, the CEMA working group must be integrated into the staff's battle rhythm. The CEMA working group is responsible for coordinating horizontally and vertically to support operations and assist the fires support element throughout the

# Cyberspace Electromagnetic Activities (CEMA) Section

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 3-5 to 3-8.

The CEMA section plans, coordinates, and integrates OCO, DCO and EW in support of the commander's intent. The CEMA section collaborates with numerous staff sections to ensure unity of effort in meeting the commander's total operational objectives such as collaborating with the G-2 or S-2 to attain situation awareness and understanding of friendly, enemy, and neutral actors operating within the AO. The CEMA section is responsible for providing regular updates to the commander and staff on OCO and other supported operations conducted in the AO. The CEMA section is responsible for synchronizing and integrating cyberspace operations and EW with the operations process and through other integrating processes. Personnel assigned to the CEMA section are the—

## Cyber Electromagnetic Warfare Officer (CEWO)

The CEWO is the commander's designated staff officer responsible for integrating, coordinating, and synchronizing actions in cyberspace and the EMS. The CEWO is responsible for understanding all applicable classified and unclassified cyberspace and spectrum-related policies to assist the commander with planning, coordinating, and synchronizing cyberspace operations, EW, and CEMA. A commander that has been delegated electromagnetic attack control authority from higher headquarters may further delegate it to the CEWO. Refer to ATP 3-12.3 for specific roles and responsibilities of the CEWO. Tasks for which the CEWO is responsible include—

- Advising the commander on effects in cyberspace (including associated rules of engagement, impacts, and constraints) in coordination with the staff judge advocate.
- Advising the commander of mission risks presented by possible cyberspace and EW vulnerabilities and adversary capabilities.
- Analyzing the OE to understand how it will impact operations within cyberspace and the EMS.
- Developing and maintaining the consolidated cyberspace and EW target synchronization matrix and recommending targets for placement on the units' target synchronization matrix.
- Assisting the G-2 or S-2 with the development and management of the electromagnetic order of battle.
- Serving as the electromagnetic attack control authority for EW missions when directed by the commander.
- Advising the commander on how cyberspace and EW effects can impact the OE.
- Receiving and integrating cyberspace and EW forces and associated capabilities into operations.
- Coordinating with higher headquarters for OCO and EW support on approved targets.
- Recommending cyberspace operations and EW-related CCIRs.
- Preparing and processing all requests for cyberspace and EW support.
- Overseeing the development and implementation of cyberspace operations and EW-related home-station training.
- Providing employment guidance and direction for organic and attached cyberspace operations and EW assets.
- Tasking authority for all assigned EW assets.

## Cyber Warfare Officer (Corps And Brigade) or Cyber Operations Officer (Division)

The cyber warfare officer (corps and brigade) or cyber operations officer (division) assists the CEWO with integrating and synchronizing cyberspace operations into the operations process and provides insight into cyberspace capabilities. The cyber warfare officer or cyber operations officer collaborates with the CEWO in vetting and processing potential targets received from subordinate units for OCO effects. The cyber warfare officer or cyber operations officer—

- Assists the CEWO in the integration, coordination, and synchronization of cyberspace operations and EW with operations.
- Provides the CEWO with information on the effects of cyberspace operations, including associated rules of engagement, impacts, and constraints used to advise the commander.
- Assists the CEWO with developing and maintaining a consolidated cyberspace target synchronization matrix and assists in nominating OCO-related targets for approval by the commander.
- Assists the CEWO in monitoring and assessing measures of performance and effectiveness while maintaining updates on cyberspace operation's effects on the OE.
- Assists the CEWO in requesting and coordinating for OCO support while integrating received cyber mission forces into operations.
- Coordinates with unified action partners for cyberspace capabilities that complement or increase the unit's cyberspace operations posture.
- Coordinates cyberspace operations with the G-2 or S-2 and the G-6 or S-6.
- Develops and implements cyberspace operations-related home station training.

## Electromagnetic Warfare Technician (EWT)

The Electromagnetic Warfare Technician (EWT) is a critical asset to the CEMA section and the EW platoon as they serve as the resident technical and tactical expert across all echelons. The EWT assist in the accomplishment of mission objectives by coordinating, integrating, and synchronizing CEMA effects to exploit and gain an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum (EMS), while simultaneously denying and degrading adversary and enemy use of the same.

*See pp. 3-11 to 3-16 for discussion of EW key personnel and duties from ATP 3-12.3.*

## Electromagnetic Warfare Sergeant Major (Corps) or NCOIC (Division)

The EW sergeant major or NCOIC is the CEWO's senior enlisted advisor for EW. The EW sergeant major or NCOIC assists the CEWO and cyber warfare officer with integrating, coordinating, and cyberspace operations and EW with operations.

*See pp. 3-11 to 3-16 for discussion of EW key personnel and duties from ATP 3-12.3.*

## Electromagnetic Warfare Noncommissioned Officer (EW NCO)

The EW NCO manages the availability and employment of EW assets assigned to the unit.

*See pp. 3-11 to 3-16 for discussion of EW key personnel and duties from ATP 3-12.3.*

## Cyberspace Electromagnetic Activities Spectrum Manager

The CEMA spectrum manager assists the CEMA section in the planning, coordination, assessment, and implementation of EW through frequency management. The CEMA spectrum manager defines the EMOE for the CEMA section.

*See chap. 5, Spectrum Management Operations.*

execution of an operation. Generally, the CEMA working group is comprised of staff representatives with equities in CEMA, and typically include—

- The G-2 or S-2.
- The G-6 or S-6.
- The IO officer or representative.
- The G-6 or S-6 spectrum manager.
- The fire support officer or a fires support element representative.
- The staff judge advocate.
- The Protection Officer.

## IV. Staff and Support at Corps and Below

During the operations process and associated integrating processes, cyberspace operations and EW require collaborative and synchronized efforts with other key staff. The G-6 or S-6 oversees DODIN operations, and the G-6 or S-6 spectrum manager collaborates with the CEMA spectrum manager to synchronize spectrum management operations with EW. The G-2 or S-2 manages the integration and synchronization of the IPB process and information collection. The IO officer oversees the integration and synchronization of information-related capabilities for IO. The staff judge advocate advises the commander on the legality of operations.

### A. Assistant Chief of Staff, Intelligence

The G-2 or S-2 provides intelligence to support CEMA. The G-2 or S-2 facilitates understanding the enemy situation and other operational and mission variables. The G-2 or S-2 staff provides direct or indirect support to cyberspace operations and EW through information collection, enabling situational understanding, and supporting targeting and IO. The G-2 or S-2 further supports CEMA by—

- Assessing CEMA intelligence and plans while overseeing information collection and analysis to support the IPB, target development, enemy COA estimates, and situational awareness.
- Continually monitoring intelligence operations and coordinating intelligence with supporting higher, lateral, and subordinate echelons.
- Coordinating SIGINT.
- Coordinating for intelligence and local law enforcement support to enhance cyberspace security.
- Leading the IPB and developing IPB products.
- Overseeing the development and management of the electromagnetic order of battle.
- Providing all-source intelligence to CEMA.
- Coordinating with the G-3 or S-3 and fires support element to identify high-value target(s) from the high-payoff target list for each friendly COA.
- Coordinating with the intelligence community to validate threat-initiated cyberspace attack or EA activities in the OE.
- Requesting intelligence support and collaborating with the intelligence community and local law enforcement to gather intelligence related to threat cyberspace operations and EW in the OE.
- Providing information and intelligence on threat cyberspace and EW characteristics that facilitate situational understanding and supports decision making.
- Coordinating with Air Force Combat Weather Forecasters for information on the terrain and weather variables for situational awareness.

- Ensuring information collection plans and operations support CEMA target development, target update requirements, and combat assessment.
- Developing requests for information and collection for information requirements that exceed the unit's organic intelligence capabilities.
- Collecting, processing, storing, displaying, and disseminating cyberspace operations and EW relevant information throughout the operations process and through command and control systems.
- Consolidating all high-value target(s) on a high-payoff target list.
- Providing input for guarded frequencies from the intelligence community.
- Providing the CEMA section and G-6 or S-6 prioritized EMS usage requirements for intelligence operations.
- Participating as a member of the CEMA working group.
- Assisting the CEMA spectrum manager in mitigating EMI and resolving EMS deconfliction and assisting with determining the source of unacceptable EMI.

## **B. Assistant Chief of Staff, Signal**

In collaboration with the joint force and unified action partners (as appropriate), the G-6 or S-6 staff directly or indirectly supports cyberspace operations by conducting DODIN operations. G-6 or S-6 is the primary staff representative responsible for spectrum management operations. The G-6 or S-6 staff supports CEMA by—

- Establishing the tactical portion of the DODIN-A, known as the tactical network, at theater army and below.
- Conducting DODIN operations activities, including cyberspace security, to meet the organization's communications requirements.
- Assisting in developing the cyberspace threat characteristics specific to enemy and adversary activities and related capabilities within friendly networks, and advising on cyberspace operations COAs.
- Conducting cyberspace security risk assessments based on enemy or adversary tactics, techniques, and procedures, identifying vulnerabilities to crucial infrastructure that may require protection measures that exceed the unit's capabilities and require DCO-IDM support.
- Participating in the CEMA working group.
- Providing a common operational picture of the DODIN for planning purposes and situational awareness.
- Providing subject matter expertise regarding wired and wireless networks.
- Ensuring security measures are configured, implemented, and monitored on the DODIN-A based on threat reports.
- Overseeing spectrum management operations.
- Implementing layered security by employing tools to provide layered cyberspace security and overseeing security training throughout the organization.
- Coordinating with the regional cyber center to ensure the unit understands and meets compliance of all cyberspace operations policies and procedures within the region.
- Requesting satellite and gateway access through the regional satellite communications support center.
- Coordinating with regional hub node to establish network connectivity and access services.



## C. G-6 or S-6 Spectrum Manager

The G-6 or S-6 spectrum manager coordinates EMS usage for various communications and electronic systems and resources. The G-6 or S-6 spectrum manager supports CEMA by—

- Coordinating spectrum resources for the organization.
- Coordinating for spectrum usage with higher headquarters, host nations, and international agencies as necessary.
- Coordinating frequency allocation, assignment, and usage.
- Coordinating spectrum resources for communications assets used for deception operations.
- Coordinating with the higher headquarters' spectrum manager to mitigate EMI identified in the unit's portion of EMOE.
- Seeking assistance from the higher the headquarters' spectrum managers for a resolution to unresolvable internal EMI.
- Participating in the CEMA working group.
- Assisting the CEMA spectrum manager with deconflicting friendly EMS requirements with planned EW, cyberspace operations, and information collection.
- Collaborating with the CEMA spectrum manager to ensure the integration and synchronization of spectrum management operations with EW.

## D. Information Operations Officer (Corps & Division) or Representative (Bde & Below)

The IO officer or representative leads the unit's IO element. The IO officer or representative contributes to the IPB by identifying and evaluating threats targeted actors in the AO. *See facing page for further discussion.*

## E. Fires Support Element

The fires support element plans, coordinates, integrates, synchronizes, and deconflicts current and future fire support to meet the commander's objectives. Fire support coordination may include collaboration with joint forces and unified action partners. The fires support element coordinates with the CEMA section to synchronize, plan, and execute cyberspace attacks and EA as part of the targeting process. The fires support element support CEMA by—

- Leading the targeting working group and participating in the targeting board chaired by the commander.
- Assisting the G-2 or S-2 with synchronizing the information collection plan with cyberspace operations, EW, and other fires.
- Collaborating with the CEMA section and the G-2 or S-2 in developing and managing the high-payoff target list, target selection standards, attack guidance matrix, and targeting synchronization matrix, all of which include cyberspace attack and EA-related targets.
- FM 3-12 provides additional bullets for FSE support to CEMA.

## F. Staff Judge Advocate

The staff judge advocate is the field representative of the Judge Advocate General and the primary legal adviser to the commander. The staff judge advocate also advises the CEMA working group concerning operational law, and the legality of cyberspace operations and EW, particularly those cyberspace and EW tasks that may affect noncombatants. The staff judge advocate is the unit's subject matter expert on the law of war, rules of engagement, the protection of noncombatants, detainee operations, and fiscal and contract law, providing commanders and staff with essential input on plans, directives, and decisions related to lethal and nonlethal targeting.

# Information Operations Officer (Corps & Division) or Representative (Bde & Below)

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 3-10 to 3-11.

The IO officer or representative leads the unit's IO element. The IO officer or representative contributes to the IPB by identifying and evaluating threats targeted actors in the AO. The IO officer or representative leads the planning, synchronization, and employment of information-related capabilities not managed by a capability owner or proponent. The IO officer or representative coordinates with the CEMA section with integrating cyberspace operations and EW into IO.

- Leading the IO working group.
- Identifying the most effective information-related capabilities to achieve the commander's objectives.
- Synchronizing cyberspace operations and EW with other information-related capabilities to achieve the commander's objectives in the information environment.
- Assessing the risk-to-mission and risk-to-force associated with employing cyberspace operations, EW, and other information-related capabilities in collaboration with the CEMA section.
- Identifying information-related capabilities gaps not resolvable at the unit level.
- Coordinating with Army, other Services, or joint forces for information-related capabilities to augment the unit's shortfalls.
- Providing information, as required, in support of OPSEC at the unit level.
- Collaborating with the CEMA section to employ cyberspace manipulation and EA deception tasks in support of military deception.
- Assessing the effectiveness and making plan modifications to employed information-related capabilities.
- Developing products that describe all military and civilian communications infrastructures and connectivity links in the AO in coordination with the G-2 or S-2.
- Locating and describing all EMS systems and emitters in the EMOE in coordination with the G-2 or S-2, CEMA section, and other information-related capabilities owners.
- Identifying network vulnerabilities of friendly, neutral, and threat forces in coordination with the G-2 or S-2, CEMA section, and other information-related capabilities owners.
- Providing understanding of information-related conditions in the OE in coordination with the G-2 or S-2.
- Participating in the military decision-making process and developing IO-related IRs.
- Participating member of the CEMA working group.
- Integrating IO into the unit's targeting process.
- Integrating non-organic information-related capabilities into operations.
- Ensuring IO-related information is updated in the common operational picture.
- Collaborating with the fire support coordinator for lethal and non-lethal effects.



Refer to INFO1: *The Information Operations & Capabilities SMARTbook (Guide to Information Operations & the IRCs)*. INFO1 chapters and topics include information operations (IO defined and described), information in joint operations (joint IO), information-related capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution (IO working group, IO weighted efforts and enabling activities, intel support), fires & targeting, and information assessment.

## V. Electromagnetic Warfare (EW) Organizations

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 3-3 to 3-4. See also 3-11 to 3-16, EW key personnel.

### Electromagnetic Warfare (EW) Platoon

EW platoons are located in the military intelligence company of a brigade combat team's brigade engineer battalion. An EW platoon consists of three EW teams with the capability to provide EW support during close operations. Though the CEMA section aligns EW and cyberspace operations with the operations process, they must collaborate with the BCT's S-2 to task the military intelligence company for deploying EW platoon assets in support of assigned EW missions.

The EW platoon performs electromagnetic reconnaissance to identify and locate enemy emitters and spectrum-dependent devices within assigned AO using sensors. Data and information attained through electromagnetic reconnaissance provide the commander with critical combat information. This data and information also supports electromagnetic battle management by providing continuous situational awareness to the CEMA spectrum manager to develop and update the common operational picture of the EMOE. An EW platoon can also conduct EA to degrade and neutralize enemy spectrum-dependent devices.

When given electromagnetic attack control authority from the JTF headquarters, the JFLCC may further delegate electromagnetic attack control authority to subordinate Army commanders. Electromagnetic attack control authority is a broader evolution of jamming control authority that enables subordinate commanders with the authority to transmit or cease transmission of electromagnetic energy. Electromagnetic attack control authority allows commanders to control EA missions conducted throughout their AO within the constraints of their higher headquarters. Before receiving electromagnetic spectrum coordinating authority, commanders should ensure they have situational awareness of the EMOE, operational control of EW capabilities, and the ability to monitor and estimate EW transmission activities within their AO to determine corrective actions when necessary. Commanders should also ensure that EW missions are thoroughly vetted to ensure deconfliction with friendly spectrum dependent devices. The G-6 spectrum management chief or the G-6 or S-6 spectrum manager is responsible for performing electromagnetic battle management for the unit.

EW platoons reprogram all assigned EW equipment according to system impact messages received from Service equipment support channels that include recommendations to respond to identified threat changes. Commanders may require an EW platoon to make immediate changes to their tactics to regain or improve EW equipment performance.

### Intelligence, Information, Cyber, Electromagnetic Warfare, and Space Detachment (I2CEWS)

The I2CEWS detachment is a battalion-sized unit assigned to a multi-domain task force and includes an enhanced CEMA section. The I2CEWS provides cyberspace operations and EW support to an Army Service Component Command, theater army, or the JTF conducting long-range precision joint strikes during multi-domain operations. The I2CEWS is composed of four companies consisting of cyberspace forces with the capability to perform Service-level DCO-IDM and EW operators capable of delivering EA effects throughout the MDTFs assigned AO.

The I2CEWS has organic sensing and intelligence, information, and space operations assets that, when integrated and synchronized with DCO-IDM and EW, allows Army forces to simultaneously defend their assigned portion of the DODIN-A while disrupting, denying, and degrading enemy EMS capabilities. The I2CEWS is structured to meet the continually changing OE in which joint operations are being conducted collaboratively and simultaneously in multiple domains.

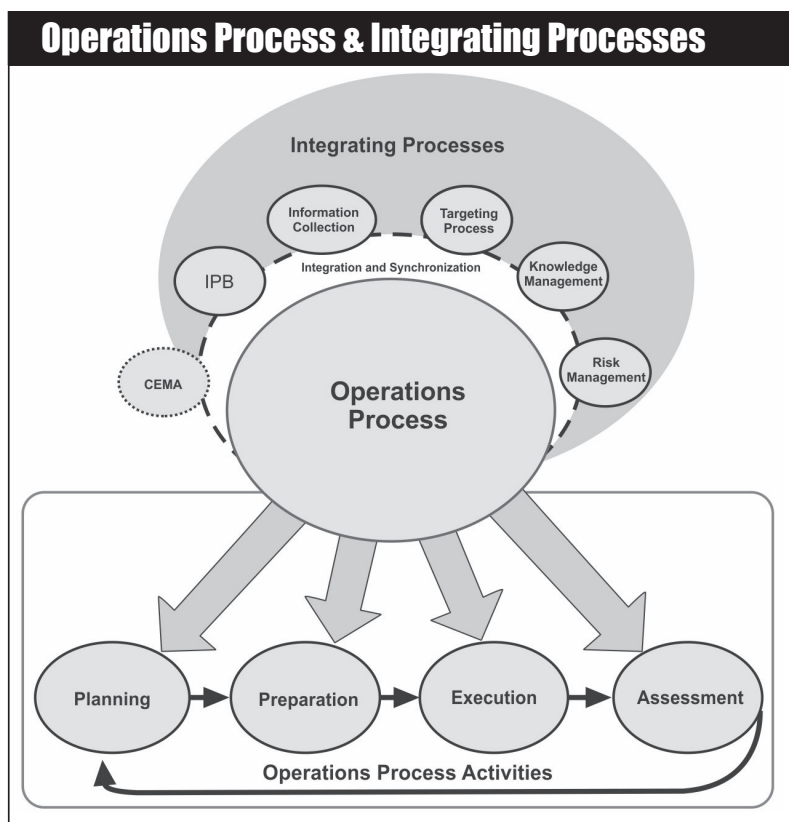
# IV. Integration through the Operations Process

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), chap. 4.

At corps and below, the planning, synchronization, and integration of cyberspace operations and EW are conducted by the CEMA section, in collaboration with key staff members that make up the CEMA working group. The CEMA section is an element of the G-3 or S-3 and works closely with members of the CEMA working group to ensure unity of effort to meet the commander's objectives.

## I. The Operations Process

The operations process includes the major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0).



Ref: FM 3-12 (Aug '21), fig. 4-1. *The operations process and integrating processes.*

The operations process is the Army's framework for the organization and implementation of command and control. The CEMA working group enables the commander with the ability to understand cyberspace and the EMOE.

Commanders, staff, and subordinate headquarters use the operations process to organize efforts, integrate the warfighting functions across multiple domains, and synchronize forces to accomplish missions. Army forces plan, prepare, execute, and assess cyberspace operations and EW in collaboration with joint forces and unified action partners as required. Army commanders and staffs will likely coordinate or interact with joint forces to facilitate cyberspace operations and EW. For this reason, commanders and staff should have an awareness of joint planning systems and processes that enable cyberspace operations and EW.

## A. Planning

Planning is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Commanders apply the art of command and the science of control to ensure cyberspace operations and EW support the concept of operations. Whether cyberspace operations and EW are planned and directed from higher headquarters or requested from tactical units, timely staff actions and commanders' involvement coupled with continued situational awareness of cyberspace and the EMS are critical for mission success.

*See chap. 4, Cyberspace and EW Planning.*

## B. Preparation

Preparation consists of those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5.0). Preparation activities include initiating information collection, DODIN operations preparation, rehearsals, training, and inspections. Preparation requires the commander, staff, unit, and Soldiers' active engagement to ensure the force is ready to execute operations.

Preparation activities typically begin during planning and continue into execution. At corps and below, subordinate units' that are task-organized to employ cyberspace operations and EW capabilities (identified in the OPLAN or OPORD) conduct preparation activities to improve the force's opportunity for success during operations. Commanders drive preparation activities through leading and assessing. Using the following preparation functions, commanders and staff can—

- **Improve situational understanding.** Commanders, staff, and subordinate units continue to refine knowledge of cyberspace and the EMOE within the assigned AO, including the improved insight on how the use of cyberspace and the EMS could affect operations across multiple domains.
- **Develop a shared understanding of the plan.** Commanders, staff, and tasked subordinate units develop a shared understanding of the plan (described in the OPLAN or OPORD) by conducting home-station training and combat training center(s). These training events provide the perfect opportunity for subordinate commanders, leaders, and Soldiers to execute the developed plan in a controlled environment and to identify issues in the developing plan that require modification.
- **Train and become proficient in critical tasks.** Through rehearsals and training, subordinate units gain and refine skills in those individual and collective tasks essential to the success of cyberspace operations and EW. Commanders also allocate training time for anticipated and unanticipated events and circumstances.
- **Integrate the force.** Commanders allocate preparation time to put the new task-organized force into effect. Integrating the force includes detaching units, moving cyberspace and EW assets, and receiving and integrating new units and Soldiers into the force. Task-organized forces require preparation time to learn the gaining unit's policies and standards and to understand their role in the overall plan. The gaining unit requires time to assess the task-organized forces' cyberspace and EW capabilities and limitations and integrate new capabilities.

- **Ensure the positioning of forces and resources.** Positioning and task organization occur concurrently. Commanders ensure cyberspace and EA assets consist of the right personnel and equipment using pre-operations checks while ensuring those assets are in the right place at the right time.

## C. Execution

Execution is the act of putting a plan into action by applying combat power to accomplish the mission (ADP 5-0). The commander, staff, and subordinate commander's focus on translating decisions made during planning and preparing into actions. Commanders conduct OCO and EA to project combat power throughout cyberspace and the EMS, conduct DCO and EP to protect friendly forces and systems, and conduct reconnaissance through cyberspace and the EMS to gather combat information for continuing situational awareness.

Commanders should understand that detailed planning provides a reasonable forecast of execution but must also be aware that situations may change rapidly in cyberspace and the EMOE. During execution, commanders take concerted action to seize, retain, and exploit operational initiative while accepting risk.

Operational initiative is the setting of tempo and terms of action throughout an operation (ADP 3-0). By presenting the enemy with multiple cross-domain dilemmas, including cyberspace and the EMS, commanders force the enemy to react continuously, driving the enemy into positions of disadvantage.

Commanders can use cyberspace attacks and EA to force enemy commanders to abandon their preferred courses of action and make costly mistakes. Commanders retain the initiative by synchronizing cyberspace attacks and EA as fires combined with other elements of combat power to apply unrelenting pressure on the enemy using continuously changing combinations of combat power at a tempo an enemy cannot effectively counter.

Commanders and staff continue to use information collection and electromagnetic reconnaissance assets to identify enemy attempts to regain the initiative. Information collected can be used to readjust targeting priorities and fire support plans, including cyberspace attacks and EA, to keep adversaries on the defensive.

Once friendly forces seize the initiative, they immediately exploit it through continued operations to accelerate the enemy's defeat. Defeat is to render a force incapable of achieving its objective (ADP 3-0). Commanders can use cyberspace attacks and EA to disrupt enemy attempts to reconstitute forces and exacerbate enemy disorganization by targeting adversary command and control and sensing nodes.

## D. Assessment

Assessment is the determination of the progress toward accomplishing a task, creating an effect, or achieving an objective (JP 3-0). The commander and staff continuously assess cyberspace operations and EW to determine if they have resulted in the desired effect. Assessment activities support decision making by ascertaining the progress of the operation to develop and refine plans.

Assessment both precedes and guides the other activities of the operations process, and there is no single way to conduct it. Commanders develop an effective assessment plan built around the unique challenges of the operations.



*Refer to BSS6: The Battle Staff SMARTbook, 6th Ed. for further discussion. BSS6 covers the operations process (ADP 5-0); commander's activities; Army planning methodologies; the military decisionmaking process and troop leading procedures (FM 7-0 w/Chg 2); integrating processes (IPB, information collection, targeting, risk management, and knowledge management); plans and orders; mission command, C2 warfighting function tasks, command posts, liaison (ADP 6-0); rehearsals & after action reviews; and operational terms and military symbols (ADP 1-02).*

## II. Integrating Processes

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 4-4 to 4-21.

Commanders and staff integrate warfighting functions and synchronize the force to adapt to changing circumstances throughout the operations process. The CEMA section aligns cyberspace operations and EW with the operations process and its associated integrating processes to identify threats in cyberspace and the EMS, to target and attack enemy cyberspace and EMS enabled systems, and to support the warfighting functions.

The operations process is the principal essential activity conducted by a commander and staff. The commander and staff integrate and synchronize CEMA with five key integrating processes throughout the operations process (see figure 4-1). These integrating processes are—

### A. Intelligence Preparation of the Battlefield (IPB)

To integrate and synchronize the tasks and missions of information collection, the G-2 or S-2 leads the staff through the IPB process. Intelligence preparation of the battlefield 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 (ATP 2-01.3). IPB assists in developing an in-depth understanding of relevant aspects of the OE, including threats.

Integrating the IPB process into the operations process is essential in supporting the commander's ability to understand the OE and visualize operations throughout the operations process. Integrating the IPB process and the operations process is an enabler that allows commanders to design and conduct operations continuously. Integrating the IPB process and the operations process provides the information and intelligence required to plan, prepare, execute, and assess operations.

See pp. 4-a to 4-4 for full discussion of IPB.

### B. Information Collection

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). These sensors and assets may include cyberspace operations and EW assets conducting cyberspace exploitation operations, electromagnetic probing, and electromagnetic reconnaissance for information collection.

Information collection is the acquisition of information and the provision of this information to processing elements. Information collection integrates the intelligence and operations staff functions with a focus on answering the CCIRs, and IRs that assists the commander and staff in shaping the OE and conducting operations. The commander drives information collection coordinated by the staff and led by the G-2 or S-2. The following are the steps of information collection:

- Plan requirements and assess collection.
- Task and direct collection.
- Execute collection.

Information collection enables the commander to understand and visualize the operation. Information collection identifies gaps in information that require aligning intelligence assets with cyberspace exploitation, electromagnetic reconnaissance, and electromagnetic probing to collect data on those gaps. The decide and detect steps of targeting also rely heavily on information collection. Enemy cyberspace capabilities identified through information collection assist the CEMA working group in identifying potential targets and key terrain in cyberspace.

See p. 2-44 for further discussion of information collection.



## C. Targeting

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). A target is an entity or object that performs a function for the adversary considered for possible engagement or other actions. (JP 3-60).

When targeting for cyberspace effects, the physical network layer is the medium through which all digital data travels. The physical network layer includes wired (land and undersea cable), and wireless (radio, radio-relay, cellular, satellite) transmission means. The physical network layer is a point of reference used during targeting to determine the geographic location of an enemy's cyberspace and EMS capabilities.

When targeting, planners may know the logical location of some targets without knowing their physical location. The same is true when defending against threats in cyberspace. Defenders may know the logical point of origin for a threat without necessarily knowing the physical location of that threat. Engagement of logical network layer targets can only occur with a cyberspace capability.

*See pp. 4-29 to 4-34, Targeting (D3A).*

## D. Risk Management

Risk management is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0) and an element of command and control. Risk is the exposure of someone or something valued to danger, harm, or loss, and is inherent in all operations. The commander and staff conduct risk management throughout the operations process to identify and mitigate risks associated with hazards that can cause friendly and civilian casualties, damage or destruction of equipment, or otherwise impact mission effectiveness. Aspects of cyberspace defense and security operations and EP missions include risk mitigation measures as part of risk management.

Risk management is integrated into planning activities and continues throughout the operations process. Risk management consists of the following steps:

- Identify the hazards.
- Assess the hazards.
- Develop controls and make risk decisions.
- Implement controls.
- Supervise and evaluate.

The CEMA section, as with all staff elements, incorporate risk management into cyberspace operations and EW-related running estimates and recommendations to mitigate risk. The G-3/S-3 coordinates risk management amongst all staff elements during the operations process.

*See following pages (pp. 2-42 to 2-43) for discussion of risks in cyberspace and the EMS.*

## E. Knowledge Management

Knowledge management is the process of enabling knowledge flow to enhance shared understanding, learning, and decision making (ADP 6-0). The four components of knowledge management are people, processes, tools, and organizations. Knowledge management facilitates the transfer of knowledge among the commander, staff, and forces to build and maintain situational awareness and enhance organizational performance. Through knowledge management, information gets to the right personnel at the right time to facilitate decision making.

During knowledge management, the necessary cyberspace operations and EW-related information and tools from higher headquarters are provided to the CEMA working group in a timely enough manner to make decisions during mission analysis and COA development. Through the knowledge management process, cyberspace operations and EW-related intelligence received through information collection and IO is disseminated for decision making by the CEMA working group.

### III. Risks In Cyberspace and the EMS

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 4-18 to 4-20.

Risk is inherent in all military operations. When commanders accept risks, they create opportunities to seize, retain, and exploit the initiative and achieve decisive results. The willingness to incur risks is often the key to exposing an enemy's weaknesses that the enemy considers beyond friendly reach. Commanders assess and mitigate risks continuously throughout the operations process. Many risks to the DODIN-A come from enemies, adversaries, and insiders. Some threats are well equipped and well trained, while some are novices using readily available and relatively inexpensive equipment and software. Army users of the DODIN are trained on basic cyberspace security, focusing on the safe use of information technology and understanding common threats in cyberspace.

Risk management is the Army's primary decision-making process for identifying hazards and controlling risks. The process applies to all types of operations, tasks, and activities, including cyberspace operations. The factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations provide a standardized methodology for addressing both threat and hazard-based risks. Risks associated with cyberspace operations fall into four major categories—

#### A. Operational Risks

Operational risks pertain to the consequences that cyberspace and EMS threats pose to mission effectiveness. Operational consequences are the measure of cyberspace attack and EA effectiveness. Cyberspace intrusions or attacks, and likewise in the EMS, can compromise networks, systems, and data, which can result in operational consequences such as injury or death of personnel, damage to or loss of equipment or property, degradation of capabilities, mission degradation, or even mission failure. Exfiltration of data from Army networks by the enemy can undermine the element of surprise and result in loss of initiative. Enemy or adversary forces may conduct cyberspace and EMS attacks to exposed friendly networks and capabilities, compromising future cyberspace attacks and cyberspace exploitation missions.

Friendly forces conducting cyberspace operations and EW encounter many operational risks. Commander and staff consider cascading effects because of employing cyberspace attacks and EA. The CEMA section ensures that the commander and staff understand the characteristics of the various cyberspace and EW capabilities and their associated effects. The CEMA section informs the commander and staff of the reversibility of effects resulting from cyberspace attacks and EA to understand that some effects are irreversible at the operator level. Attaining an understanding of the characteristics, cascading effects, and reversibility effects provide a commander with situational awareness and in determining the acceptable risks when conducting cyberspace operations and EW.

It is essential to consider risk management when conducting OCO and EA that could reveal friendly locations and intentions to an adversary prematurely. Some OCO or EA effects have a one-time use and once utilized cannot be effectively used again. OCO and EA may also create cascading effects that could hinder other operations.

Personal electronic device(s) such as smartwatches, smartphones, tablets, laptops, and gaming systems can be a significant OPSEC vulnerability to friendly cyberspace and EW capabilities. The CEWO gathers understanding surrounding risks associated with PEDs from the G2 or S2 and OPSEC and makes recommendations to the commander regarding their usage in the organization.

#### B. Technical Risks

Technical risks exist when there are exploitable vulnerabilities in systems on the DODIN-A, and there are threats that can exploit those vulnerabilities. Nearly every technical sys-

tem within the Army is networked, resulting in a vulnerability in one system compromising other connected systems, creating a shared vulnerability. These potentially vulnerable networked systems and components directly impact the Army's ability to conduct operations. DCO mitigates risks by defending against specified cyberspace attacks, thereby denying the enemy's ability to take advantage of technical vulnerabilities that could disrupt operations.

Robust information systems engineering disciplines result in chain risk management, security, counterintelligence, intelligence, and hardware and software assurance that assist the leaders with managing technical risk. Friendly forces examine the technical risks when conducting cyberspace attacks to avoid making friendly networks vulnerable to enemy cyberspace counterattacks.

## C. Policy Risks

Policy risk pertains to authorities, legal guidance, and international law. Policies address cyberspace boundaries, authorities, and responsibilities. Commanders and decision makers must perform risk assessments and consider known probable cascading and collateral effects due to overlapping interests between military, civil, government, private, and corporate activities on shared networks in cyberspace. Policies, the United States Code (USC), the Uniform Code of Military Justice, regulations, publications, operation orders, and standard operating procedures all constitute a body of governance for making decisions about activities in cyberspace.

Policy risk includes considering international norms and practices, the effect of deviating from those norms, and potential shifts in international reputation because of the effects resulting from a cyberspace operation. Cyberspace attacks can be delivered through networks owned, operated, and geographically located within the sovereignty of multiple governments. EA can also deliver effects that impact frequencies in the spectrum owned and operated by commercial, government, and other neutral users. Therefore, it is vital to consider the legal, cultural, and political costs associated with using cyberspace and the EMS as avenues of approach.

Policy risks occur where policy fails to address operational necessity. For example, a policy enacted that limits cyberspace operations, which results in low levels of collateral effects, can result in a unit constrained to cyberspace attacks that will not result in the desired outcomes necessary for mission success. A collateral effects analysis to meet policy limits is distinct from the proportionality and necessity analysis required by the law of war. Even if a proposed cyberspace operation is permissible after a collateral effect's analysis, the proposed cyberspace operation or EW mission must include a legitimate military objective that is also permissible under the law of war.

Policy risk applies to risk management under civil or legal considerations. An OCO or EA mission may pose a risk to host nation civilians and non-combatants in an OE where a standing objective is to minimize collateral damage. During a mission, it may be in the Army's best interest for host nation populations to be able to perform day-to-day activities. Interruptions of public networks may present hazards to the DODIN-A and pose dangers to Army forces because of social impacts that lead to riots, criminal activity, and the emergence of insurgent opportunists seeking to exploit civil unrest.

## C. Operations Security Risks

Both cyberspace and the EMS provides a venue for OPSEC risks. The Army depends on cyberspace security programs and training to prevent or mitigate OPSEC risks. Commanders emphasize and establish OPSEC programs to minimize the risks. OPSEC measures include actions and information on the DODIN and non-DODIN information systems and networks. All personnel are responsible for protecting sensitive and critical information. EP denies unauthorized access to information that an enemy intercept in the EMS through electromagnetic security operations.

*For more information on OPSEC, refer to AR 530-1 and ATP 3-13.3.*

# Information Collection

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 4-9 to 4-10. See also p. 2-40.

The focus when executing information collection is to collect data that answers CCIRs and IRs for analysis during the IPB process. The G-2 or S-2 executes collection by conducting—

**Intelligence Operations.** Intelligence operations are the tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements (ADP 2-0). Through intelligence operations, the G-2 or S-2 attains information regarding threat capabilities, activities, disposition, and characteristics. Intelligence operations use multiple intelligence disciplines to collect information regarding cyberspace and the EMS to satisfy CCIRs and IRs. However, knowledge attained from the other intelligence disciplines may also provide cyberspace and EMS related insight. In addition to gathering information on peer and near-peer threats through SIGINT, criminal intelligence collects information on cyberspace and EMS-related illegal activities conducted throughout the assigned AO.

**Reconnaissance.** Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (JP 2-0). Reconnaissance produces information about the assigned AO. Through reconnaissance, the G-2 or S-2 can collect information regarding such mission and operational variables as terrain characteristics, enemy and friendly obstacles to movement, and the disposition of enemy forces and civilians. Combined employment of three methods of reconnaissance (dismounted, mounted, and aerial) can result in the location and type(s) of friendly, civilian, and threat cyberspace and EW capabilities operating in the assigned AO. Upon request, the CEMA section supports the G-2 or S-2's reconnaissance efforts by employing EW assets to conduct electromagnetic reconnaissance to collect information in the EMS and request OCO support to conduct cyberspace exploitation in cyberspace.

**Surveillance.** Surveillance is the systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means (JP 3-0). Surveillance involves observing an area to collect information and monitoring civilians and threats in a named area of interest or target area of interest. Surveillance may be autonomous or part of a reconnaissance mission. Collecting information in cyberspace and the EMS as part of a surveillance mission is also called network surveillance. Network Surveillance is the observation of organizational, social, communications, cyberspace, or infrastructure connections and relationships (FM 2-0). Network surveillance can also include detailed information on connections and relationships among individuals, groups, and organizations, and the role and importance of aspects of physical or virtual infrastructure.

**Security Operations.** Security operations are those operations performed by commanders to provide early and accurate warning of enemy operations, to provide the forces being protected with time and maneuver space within which to react to the enemy and to develop the situation to allow commanders to effectively use their protected forces (ADP 3-90). Early and accurate warnings provide friendly forces with time and maneuverability to react and create an opportunity for the commander to employ force protection measures. Cyberspace defense, cyberspace security, and EP include actions that allow early detection and mitigation of threats in cyberspace and the EMS. Additionally, ES missions conduct electromagnetic reconnaissance to attain information about the disposition of enemy threats in the EMS and modify security efforts.

# I. Electromagnetic Warfare (EW)

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 2-8 to 2-15.

## I. Electromagnetic Warfare (EW)\*

**Electromagnetic Warfare (EW)** is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three functions: electromagnetic attack, electromagnetic protection, and electromagnetic support.

Modern militaries rely on communications equipment using broad portions of the electromagnetic spectrum (EMS) to conduct military operations allowing forces to talk, transmit data, and provide navigation and timing information, and command and control troops worldwide. They also rely on the EMS for sensing and awareness of the OE. The Army conducts electromagnetic warfare (EW) to gain and maintain positions of relative advantage within the EMS. The Army's contribution to electromagnetic spectrum operations is accomplished by integrating and synchronizing EW and spectrum management operations.

### Electromagnetic Warfare (EW)



**Electromagnetic Attack (EA)**



**Electromagnetic Protection (EP)**



**Electromagnetic Support (ES)**



**Electromagnetic Warfare Reprogramming**

The three divisions often mutually support each other in operations. For example, radar-jamming EA can serve a protection function for friendly forces to penetrate defended airspace; it can also prevent an adversary from having a complete operating picture.

*\* Editor's Note: In keeping with doctrinal terminology changes in JP 3-85, Joint Electromagnetic Spectrum Operations (May '20) and FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), the term "electronic warfare (EW)" has been updated to "electromagnetic warfare (EW)". Likewise, the EW divisions have been updated as "electromagnetic attack (EA), electromagnetic protection (EP), and electromagnetic support (ES)." For purposes of the CYBER1 SMARTbook, EW/EA/EP/ES acronyms and terms will remain the same as presented in the original cited and dated source -- for example, ATP 3-12.3, Electronic Warfare Techniques (Jul '19). Readers should anticipate that as those specific references are updated/revised, so will the terms.*

## A. Electromagnetic Attack (EA)

Army forces conduct both offensive and defensive EA to fulfill the commander's objectives in support of the mission. EA projects power in and through the EMS by implementing active and passive actions to deny enemy capabilities and equipment, or by employing passive systems to protect friendly capabilities. Electromagnetic attack is a 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 considered a form of fires (JP 3-85). EA requires systems or weapons that radiate electromagnetic energy as active measures and systems that do not radiate or re-radiate electromagnetic energy as passive measures.

### Offensive EA

Offensive EA prevents or reduces an enemy's effective use of the EMS by employing jamming and directed energy weapon systems against enemy spectrum-dependent systems and devices. Offensive EA systems and capabilities include—

- Jammers.
- Directed energy weaponry.
- Self-propelled decoys.
- Electromagnetic deception.
- Antiradiation missiles.

### Defensive EA

Defensive EA protects against lethal attacks by denying enemy use of the EMS to target, guide, and trigger weapons that negatively impact friendly systems. Defensive EA supports force protection, self-protection and OPSEC efforts by degrading, neutralizing, or destroying an enemy's surveillance capabilities against protected units. Defensive EA systems and capabilities include—

- Expendables (flares and active decoys).
- Jammers.
- Towed decoys.
- Directed energy infrared countermeasure systems.
- Radio controlled improvised explosive device (RCIED) systems.
- Counter Unmanned Aerial Systems (C-UAS).

### Electromagnetic Attack (EA) Effects

EA effects available to the commander include—

- **Destroy.** Destruction makes the condition of a target so damaged that it can neither function nor be restored to a usable condition in a timeframe relevant to the current operation. When used in the EW context, destruction is the use of EA to eliminate targeted enemy personnel, facilities, or equipment (JP 3-85).
- **Degrade.** Degradation reduces the effectiveness or efficiency of an enemy EMS-dependent system. The impact of degradation may last a few seconds or remain throughout the entire operation (JP 3-85).
- **Disrupt.** Disruption temporarily interrupts the operation of an enemy EMS dependent system (JP 3-85).
- **Deceive.** Deception measures are designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce them to react in a manner prejudicial to their interests. Deception in an EW context presents enemy operators and higher-level processing functions with erroneous inputs, either directly through the sensors themselves or through EMS-based networks such as voice communications or data links (JP 3-85).

# II. Electromagnetic Warfare Taxonomy

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), p. 2-8.

Electromagnetic warfare (EW) consists of three distinct divisions: electromagnetic attack (EA), electromagnetic protection (EP), and electromagnetic support (ES).

Divisions of Cyberspace Operations	Electromagnetic Attack (EA)	Electromagnetic Protection (EP)	Electromagnetic Support (ES)
Types of Operations	Attack personnel, facilities, or equipment	Protect friendly Electromagnetic Spectrum (EMS)-dependent capabilities	<ul style="list-style-type: none"><li>• Intercept</li><li>• Identify</li><li>• Locate</li><li>• Evaluate</li></ul>
Types of Enabling Operations	<ul style="list-style-type: none"><li>• Reconnaissance</li><li>• Enemy Attack</li></ul>	Preemptive Protection	<ul style="list-style-type: none"><li>• Situational Understanding</li><li>• Combat Information</li><li>• Targeting</li><li>• Intelligence Preparation of Battlespace (IPB) Development</li></ul>
Common Tactical Mission Tasks	<ul style="list-style-type: none"><li>• Employing Directed Energy Weapons</li><li>• Electromagnetic Pulse</li><li>• Reactive Countermeasures</li><li>• Deception Measures</li><li>• Electromagnetic Intrusion</li><li>• Electromagnetic Jamming</li><li>• Electromagnetic Probing</li><li>• Meaconing</li></ul>	<ul style="list-style-type: none"><li>• Deconflict Electromagnetic Environmental Effects</li><li>• Ensure Electromagnetic Compatibility</li><li>• Electromagnetic Hardening</li><li>• Emission Control</li><li>• Electromagnetic Masking</li><li>• Preemptive Countermeasures</li><li>• Electromagnetic Security</li><li>• Conduct Wartime Reserve Modes</li></ul>	<ul style="list-style-type: none"><li>• Conduct Electromagnetic Reconnaissance</li><li>• Threat Warning</li><li>• Direction Finding</li></ul>
Common Effects	<ul style="list-style-type: none"><li>• Disrupt</li><li>• Degrade</li><li>• Neutralize</li><li>• Destroy</li><li>• Deceive</li></ul>	<ul style="list-style-type: none"><li>• Deception</li><li>• Denial</li><li>• Disrupt</li><li>• Neutralize</li></ul>	<ul style="list-style-type: none"><li>• Exploit</li><li>• Detect</li></ul>

Ref: FM 3-12 (Aug '21), fig. 2-3. Electromagnetic warfare taxonomy.



# Electromagnetic Attack (EA) Tasks

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 2-9 to 2-11. See also pp. 3-21 to 3-28 for electronic attack techniques from ATP 3-12.3.

EA has the unique potential to affect enemy use of the EMS and attack the enemy through the EMS. Other offensive options can affect enemy use of the EMS but are likely to cause collateral damage outside the EMS, whereas EA uses the EMS for its effects. Concurrently, EA's potential to cause EMS fratricide necessitates caution and coordination in its employment.

EA tasks include—

- Employing directed energy weaponry.
- Electromagnetic pulse.
- Reactive countermeasures.
- Deception measures.
- Electromagnetic intrusion.
- Electromagnetic jamming.
- Electromagnetic probing.
- Meaconing.

**Directed Energy.** Directed energy is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. (JP 3-85). Directed energy becomes a directed energy weapon when used to conduct EA. A directed-energy weapon is a weapon or system that uses directed energy to incapacitate, damage, or destroy enemy equipment, facilities, and/or personnel (JP 3-85). EA involving the use of directed-energy weapons is called directed-energy warfare. Directed-energy warfare is military action involving the use of directed-energy weapons, devices, and countermeasures (JP 3-85). The purpose of directed-energy warfare is to disable, cause direct damage, or destroy enemy equipment, facilities, or personnel. Another use for directed-energy warfare is to determine, exploit, reduce, or prevent hostile use of the EMS by neutralization or destruction.

**Electromagnetic Pulse.** 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). The effects of an electromagnetic pulse can extend hundreds of kilometers depending on the height and power output of the electromagnetic pulse burst. A high-altitude electromagnetic pulse can generate destructive effects over a continent-sized area. The most affected portion of the EMS by electromagnetic pulse or high-altitude electromagnetic pulse is the radio spectrum. Electromagnetic energy produced by an electromagnetic pulse excludes the highest frequencies of the optical (infrared, visible, ultraviolet) and ionizing (X and gamma rays) ranges. An indirect impact of an electromagnetic pulse or high-altitude electromagnetic pulse includes electrical fires caused by the overheating of electrical systems and components.

**Reactive Countermeasures.** EA includes reactive countermeasures as a response to an enemy attack in the EMS. Response to enemy attack may include employing radio frequency countermeasures, such as flares and chaff, in disrupting enemy systems and weapons, such as precision-guided or radio-controlled weapons, communications equipment, and sensor systems. Radio frequency countermeasures are any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided and sensor systems (JP 3-85). Chaff is radar confusion reflectors,

consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion purposes (JP 3-85). Reactive countermeasures may provoke the employment of directed energy weaponry or electromagnetic pulse and can include the use of lethal fires. Army forces can disrupt enemy guided weapons and sensor systems by deploying passive and active electro-optical-infrared countermeasures that include smokes, aerosols, signature suppressants, decoys, pyrotechnics, pyrophoric, laser jammers, high-energy lasers, and directed infrared energy.

**Deception Measures.** Deception measures are designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce them to react in a manner prejudicial to their interests. Electromagnetic deception uses misleading information by injecting false data into the adversary's EMS-dependent voice and data networks to inhibit the effectiveness of intelligence, surveillance, and reconnaissance sensor systems. EW uses the EMS to deceive a threat's decision loop, making it difficult to establish an accurate perception of Army forces' objective reality. EW supports all deceptions plans, both Joint military deception and tactical deception, using electromagnetic deception measures and scaling appropriately for the desired effect. Electromagnetic deception measures provide misleading signals in electromagnetic energy, for example by injecting false signals into a threat's sensor systems such as radar. Commander's authority to plan and execute deception integrated with electromagnetic deception measures may be limited by separate EW authorities and rules of engagement.

**Electromagnetic Intrusion.** 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). An example of electromagnetic intrusion is injecting false or misleading information into an enemy's radio communications, acting as the enemy's higher headquarters. Electromagnetic intrusion can also create deception or confusion in a threat aircraft's intelligent flight control system, compromising the intelligent flight control system's neural network and the pilot's ability to maintain control.

**Electromagnetic Jamming.** 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). Targets subjected to jamming may include radios, navigational systems, radars, and satellites. Electromagnetic jamming can disrupt a threat aircraft's intelligent flight control system by jamming its sensors, denying its ability to obtain navigational or altitude data crucial to flight performance. Electromagnetic jamming can also prevent or reduce the effectiveness of an enemy's integrated air defense system by jamming its anti-aircraft sensors used for targeting.

**Electromagnetic Probing.** Electromagnetic probing is the 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 involves accessing an enemy's spectrum-dependent devices to obtain information about the targeted devices' functions, capabilities, and purpose. Electromagnetic probing may provide information about threat capabilities and their ability to affect or detect friendly operations. Army forces may conduct overt electromagnetic probing to elicit a response from an enemy, exposing their location.

**Meaconing.** Meaconing consists of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. Meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations (JP 3-85).

## B. Electromagnetic Protection (EP)

*Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), pp. 2-11 to 2-13. See also pp. 3-29 to 3-34 for electronic protection techniques from ATP 3-12.3.*

Electromagnetic protection is the division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-85). EP measures eliminate or mitigate the negative impact resulting from friendly, neutral, enemy, or naturally occurring EMI.

### Electromagnetic Protection (EP) Tasks

Adversaries are heavily invested in diminishing our effective use of the electromagnetic spectrum. It is crucial we understand the enemy threat and our vulnerabilities to our systems, equipment and personnel. Effective EP measures will minimize natural phenomena and mitigate the enemy's ability to conduct ES and EA actions against friendly forces successfully.

EP tasks include—

- Electromagnetic environmental effects deconfliction.
- Electromagnetic compatibility.
- Electromagnetic hardening.
- Emission control.
- Electromagnetic masking.
- Preemptive countermeasures.
- Electromagnetic security.
- Wartime reserve modes.

### Electromagnetic Environmental Effects Deconfliction.

Electromagnetic vulnerability is the characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of electromagnetic environmental effects (JP 3-85). Any system operating in the EMS is susceptible to electromagnetic environmental effects. Any spectrum-dependent device exposed to or having electromagnetic compatibility issues within an EMOE may result in the increased potential for such electromagnetic vulnerability as safety, interoperability, and reliability issues. Electromagnetic vulnerability manifests when spectrum-dependent devices suffer levels of degradation that render them incapable of performing operations when subjected to electromagnetic environmental effects.

Electromagnetic compatibility, EMS deconfliction, electromagnetic pulse, and EMI mitigation reduce the impact of electromagnetic environmental effects. Recognizing the different types of electromagnetic radiation hazards allows planners to use appropriate measures to counter or mitigate electromagnetic environmental effects. Electromagnetic radiation hazards include— hazards of electromagnetic radiation to personnel, hazards of electromagnetic radiation to ordnance, and hazards of electromagnetic radiation to fuels. Electromagnetic environmental effects can also occur from natural phenomena such as lightning and precipitation static.

**Electromagnetic Compatibility.** 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). The CEMA spectrum manager assists the G-6 or S-6 spectrum manager with implementing electromagnetic compatibility to mitigate electromagnetic vulnerabilities by applying sound spectrum planning, coordination, and management of the EMS. Operational forces have minimal ability to mitigate

electromagnetic compatibility issues. Instead, they must document identified electromagnetic compatibility issues so that the Service component program management offices may coordinate the required changes necessary to reduce compatibility issues.

**Electromagnetic Hardening.** Electromagnetic hardening consists of actions 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 hardening can protect friendly spectrum-dependent devices from the impact of EMI or threat EA such as lasers, high-powered microwave, or electromagnetic pulse. An example of electromagnetic hardening includes installing electromagnetic conduit consisting of conductive or magnetic materials to shield against undesirable effects of electromagnetic energy.

**Emission Control.** 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). emission control enables OPSEC by—

- Decreasing detection probability and countering detection range by enemy sensors.
- Identifying and mitigating EMI among friendly spectrum-dependent devices
- Identifying enemy EMI that allows execution of military deception planning.

Emission control enables electromagnetic masking by integrating intelligence, and EW to adjust spectrum management and communications plans. A practical and disciplined emission control plan, in conjunction with other EP measures, is a critical aspect of good OPSEC. *Refer to ATP 3-13.3 for OPSEC techniques at division and below.*

**Electromagnetic Masking.** 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 military operations information or present false perceptions to adversary commanders. Electromagnetic masking is an essential component of military deception, OPSEC, and signals security.

**Preemptive Countermeasures.** Countermeasures consist of that form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity (JP 3-85). Countermeasures can be passive (non-radiating or reradiating electromagnetic energy) or active (radiating electromagnetic energy) and deployed preemptively or reactively. Preemptive deployment of passive countermeasures are precautionary procedures to disrupt an enemy attack in the EMS through the use of passive devices such as chaff which reradiates, or the use of radio frequency absorptive material which impedes the return of the radio frequency signal.

**Electromagnetic Security.** Electromagnetic security is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiation (e.g., radar) (JP 3-85). Changing the modulation and characteristics of electromagnetic frequencies used for radars make it difficult for a threat to intercept and study radar signals.

**Wartime Reserve Modes.** Wartime reserve modes are characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasure systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance (JP 3-85). Wartime reserve modes are held deliberately in reserve for wartime or emergency use.

## C. Electromagnetic Support (ES)

Electromagnetic support refers to the division of electromagnetic warfare involving actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conduct of future operations (JP 3-85). In multi-domain operations, commanders work to dominate the EMS and shape the operational environment by detecting, intercepting, analyzing, identifying, locating, and affecting (deny, degrade, disrupt, deceive, destroy, and manipulate) adversary electromagnetic systems that support military operations. Simultaneously, they also work to protect and enable U.S. and Allied forces' freedom of action in and through the EMS.

The purpose of ES is to acquire adversary combat information in support of a commander's maneuver plan. Combat information is unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements (JP 2-01). Combat information used for planning or conducting combat operations, to include EA missions, is acquired under Command authority; however, partner nation privacy concerns must be taken into account. Decryption of communications is an exclusively SIGINT function and may only be performed by SIGINT personnel operating under Director, National Security Agency and Chief, National Security Service SIGINT operational control (DODI O-3115.07).

ES supports operations by obtaining EMS-derived combat information to enable effects and planning. Combat information is collected for immediate use in support of threat recognition, current operations, targeting for EA or lethal attacks, and support the commander's planning of future operations. Data collected through ES can also support SIGINT processing, exploitation, and dissemination to support the commander's intelligence and targeting requirements and provide situational understanding. Data and information obtained through ES depend on the timely collection, processing, and reporting to alert the commander and staff of potential critical combat information.

### Electromagnetic Support (ES) Tasks

When conducting electromagnetic support, commanders employ EW platoons located in the brigade, combat team (BCT) military intelligence company (MICO) to support with information collection efforts, survey of the EMS, integration and multisource analysis by providing indications and warning, radio frequency direction finding and geolocation of threat emissions.

ES tasks include—

- Electromagnetic Reconnaissance.
- Threat Warning.
- Direction finding.

*See facing page for an overview and further discussion of electronic support actions.*

## \* Electromagnetic Warfare Reprogramming

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 and targeting sensing systems. EW reprogramming includes changes to EW and targeting sensing software (TSS) equipment such as self-defense systems, offensive weapons systems, and intelligence collection systems. EW consists of three distinct divisions: EA, EP, and ES, which are supported by EW reprogramming activities.

*For more information on EW reprogramming, refer to FM 3-12, app. F.*

### \* 3-8 (Electromagnetic Warfare) I. EW Overview

# Electromagnetic Support (ES) Actions

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 2-14 to 2-15. See also pp. 3-35 to 3-36 for electronic warfare support techniques from ATP 3-12.3.

**Electromagnetic Reconnaissance.** Electromagnetic reconnaissance is the detection, location, identification, and evaluation of foreign electromagnetic radiations (energy) (JP 3-85). Electromagnetic reconnaissance is an action used to support information collection and is an element of the tactical task reconnaissance (see Chapter 4). Information obtained through electromagnetic reconnaissance assists the commander with situational understanding and decision making and, can be further processed to support SIGINT activities. Electromagnetic reconnaissance may result in EP modifications or lead to an EA or lethal attack.

**Threat Warning.** Threat warning enables the commander and staff to quickly identify immediate threats to friendly forces and implement EA or EP countermeasures. EW personnel employ sensors to detect, intercept, identify, and locate adversary electromagnetic signatures and provides an early warning of an imminent or potential threat. EW personnel coordinate with G-2 or S-2 on the long-term impact of detected enemy emitters. Threat warning assists the commander's decision making process in IPB development, updating electromagnetic order of battle, and assisting in the correlation of enemy emitters to communication and weapon systems.

Known electromagnetic signatures should be compared against the electromagnetic order of battle, high-value target, and the high-payoff target list and action taken as warranted by current policy or higher guidance. Unknown radiated electromagnetic signatures detected in the EMS are forwarded to the G-2 or S-2 for analysis. The G-2 or S-2 validates known and unknown systems as part of information collection that feeds the operations process. Staffs analyze and report information to higher and subordinate headquarters, to other Army and joint forces, and to unified action partners in the AO.

**Direction Finding.** Direction finding is a procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment (JP 3-85). EW personnel leverage various ES platforms with direction finding capabilities to locate enemy forces. Multiple direction finding systems are preferred for a greater confidence level of the enemy location. ES platforms are deployed in various formations to create a baseline and increase the area of coverage. Three or more direction finding systems are considered optimal in triangulating the targeted emitter.

## Electromagnetic Support and Signals Intelligence

ES and SIGINT often share the same or similar assets and resources, and personnel conducting ES could be required to collect information that meets both requirements simultaneously. SIGINT consists of communications intelligence, electronic intelligence, and foreign instrumentation SIGINT. Commonalities between ES and SIGINT are similar during the early stages of sensing, collecting, identifying, and locating foreign spectrum emissions. The distinction between ES and SIGINT is determined by who has operational control of assets collecting information, what capabilities those assets must provide, and why they are needed. Information and data become SIGINT when cryptologic processes are applied to a signal to determine its relevance, value, or meaning solely for intelligence. There are also delineating hard lines regarding the systems, signal complexity, and reporting timeliness that divide ES and SIGINT. While both ES and SIGINT report information that meets reporting thresholds directly to the supported unit, SIGINT is obligated further to report acquired information through the U.S. SIGINT system. The added requirement for SIGINT provides accountability and enables the greater intelligence community access to the information for additional intelligence production and dissemination as required.

### III. Spectrum Management

Spectrum management is the operational, engineering, and administrative procedures to plan, coordinate, and manage use of the electromagnetic spectrum and enables cyberspace, signal and EW operations. Spectrum management includes frequency management, host nation coordination, and joint spectrum interference resolution. Spectrum management enables spectrum-dependent capabilities and systems to function as designed without causing or suffering unacceptable electromagnetic interference. Spectrum management provides the framework to utilize the electromagnetic spectrum in the most effective and efficient manner through policy and procedure. See chap. 5, *Spectrum Management Operations (SMO/JEMSO)*.

#### Electromagnetic Interference (EMI)

Electromagnetic interference is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment (JP 3-13.1). It can be induced intentionally, as in some forms of EW, or unintentionally, because of spurious emissions and responses, intermodulation products, and other similar products. See p. 3-36 for related discussion of EMI mitigation, to include an operator EMI troubleshooting checklist. See also p. 3-31.

#### Frequency Interference Resolution

Interference is the radiation, emission, or indication of electromagnetic energy (either intentionally or unintentionally) causing degradation, disruption, or complete obstruction of the designated function of the electronic equipment affected. The reporting end user is responsible for assisting the spectrum manager in tracking, evaluating, and resolving interference. Interference resolution is performed by the spectrum manager at the echelon receiving the interference. The spectrum manager is the final authority for interference resolution. For interference affecting satellite communications, the Commander, Joint Functional Component Command for Space is the supported commander and final authority of satellite communications interference.

#### Spectrum Management Operations (SMO)

SMO are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. The SMO functional area is ultimately responsible for coordinating EMS access among civil, joint, and multinational partners throughout the operational environment. The conduct of SMO enables the commander's effective use of the EMS. The spectrum manager at the tactical level of command is the commander's principal advisor on all spectrum related matters. See chap. 5, *Spectrum Management Operations (SMO/JEMSO)*.

#### Electromagnetic Warfare Coordination

The spectrum manager should be an integral part of all EW planning. The SMO assists in the planning of EW operations by providing expertise on waveform propagation, signal, and radio frequency theory for the best employment of friendly communication systems to support the commander's objectives. The advent of common user "jammers" has made this awareness and planning critical for the spectrum manager. In addition to jammers, commanders and staffs must consider non-lethal weapons that use electromagnetic radiation. Coordination for EW will normally occur in the CEMA section. It may occur in the EW cell if it is operating under a joint construct or operating at a special echelon.



# II. EW Key Personnel

*Ref: ATP 3-12.3, Electronic Warfare Techniques (Jul '19), chap. 2.*

The conduct of electronic warfare requires highly trained and skilled personnel. This section discusses electronic warfare professionals along with the staff members with roles and responsibilities when planning and conducting electronic warfare operations.

## I. Electronic Warfare Personnel

EW personnel on the staff are in the cyberspace electromagnetic activities (CEMA) section at theater army through brigade and consist of a cyber electronic warfare officer (CEWO), electronic warfare technician, electronic warfare noncommissioned officers, and spectrum manager. The CEMA section includes EW trained personnel, personnel trained in electromagnetic spectrum management, and personnel trained in cyberspace operations. Cyberspace electromagnetic activities is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADRP 3-0). EW personnel are responsible to the chief of staff or the assistant chief of staff, operations (G-3) or battalion or brigade operations staff officer (S-3) staff. Battalions have a single EW representative that is a member of the battalion staff.

EW personnel in the CEMA section plan and conduct EW during the full range of military operations. EW personnel conduct CEMA with assistance from, and in coordination with, other members of the CEMA working group. FM 3-12 contains more information on the CEMA working group. EW personnel plan the employment of EA, frequencies for targeting, analyze the probability of frequency fratricide, and collaborate with the assistant chief of staff, signal (G-6) or battalion or brigade signal staff officer (S-6) to mitigate harmful effects from EW to friendly personnel, equipment, and facilities.

The CEWO disseminates key mission status information, such as cancellation of electronic attacks, and coordinates with other staff members within the command post to contribute to situational awareness. The CEWO coordinates with the following sections—

- Assistant chief of staff, intelligence (G-2) or battalion or brigade intelligence staff officer (S-2).
- G-3 (S-3).
- G-5 (S-5).
- G-6 (S-6).
- Fire support coordinator.
- Information operations officer.
- Space support element.
- Special technical operations staff.
- Staff Judge Advocate (SJA) or representative.

## II. Theater Army, Corps, Division and Brigade

The Army assigns EW personnel to CEMA sections at theater army, corps, division, and brigade echelons. Each EW professional has specific roles and responsibilities.

## A. Cyber Electronic Warfare Officer (CEWO)

The CEWO's EW responsibilities include—

- Integrates, coordinates, and synchronizes EW effects.
- Nominates EW targets for approval from the fire support coordinator and commander.
- Receives, vets, and processes EW targets from subordinate units.
- Develops and prioritizes effects in the EMS.
- Develops and prioritizes targets with the fire support coordinator.
- Monitors and continually assesses measures of performance and measures of effectiveness for EW operations.
- Coordinates targeting and assessment collection with higher, adjacent, and subordinate organizations or units.
- Advises the commander and staff on plan modifications, based on the assessment.
- Advises the commander on how EW effects can impact the operational environment.
- Provides recommendations on commander's critical information requirements.
- Prepares and processes the electronic attack request format (EARF).
- Participates in other cells and working groups, as required, to ensure integration of EW operations.
- Deconflicts EW operations with the spectrum manager.
- Coordinates with the CEMA working group to plan and synchronize EW operations.
- Assists the G-2 (S-2) during intelligence preparation of the battlefield (IPB), as required.
- Provides information requirements to support planning, integration, and synchronization of EW operations.
- Serves as the Jam Control Authority (JCA) for EW operations, as directed by the commander.

## B. Electronic Warfare Technician

The electronic warfare technician—

- Serves as the technical subject-matter expert for EW to the CEWO and CEMA working group.
- Plans and coordinates EW across functional and integrating cells.
- Provides input for the integration of threat electronic technical data as part of the IPB process.
- Coordinates target information and synchronizes EA and ES activities with the G-2 (S-2) staff.
- Integrates EW into the targeting process, monitors EW target requests, and conducts battle damage assessment for EW.
- Recommends employment of EW resources.
- Provides technical oversight and supervision for maintenance of EW equipment.
- Conducts, maintains, and updates an electromagnetic environment survey.
- Identifies enemy and friendly effects within the EMS.
- Assists in the development and execution of standard operating procedure (SOP) and battle drills.

## C. Electronic Warfare Noncommissioned Officer

The electronic warfare noncommissioned officer—

- Plans, manages, and executes EW tasks.
- Manages the availability and employment of EW assets.
- Serves as senior developer and trainer for EW.
- Distributes, maintains, and consolidates EW staff products.
- Collects and maintains data for electromagnetic energy surveys.
- Coordinates and deconflicts EMS resources with the spectrum manager.
- Operates and maintains EW tools.

## D. Spectrum Manager

There are spectrum managers in the CEMA section and G-6 (S-6) staff. The G-6 (S-6) staff spectrum manager manages EMS resources that support the friendly use of the EMS. The CEMA section spectrum manager manages EMS resources for EW activities and provides the EW input to the common operational picture. The CEMA section spectrum manager is responsible for—

- Leads, develops, and synchronizes the EW and EP plan by assessing EA effects on friendly force emitters.
- Mitigates harmful impact of EA on friendly forces through coordination with higher and subordinate units.
- Synchronizes with intelligence on the EA effects to support intelligence gain and loss considerations.
- Synchronizes cyberspace operations to protect radio frequency enabled transport layers.
- Coordinates to support protecting radio frequency-enabled information operations.
- Collaborates with staff, subordinate, and senior organizations to identify unit emitters for inclusion on the joint restricted frequency list (JRFL).
- Performs EW-related documentation and investigation of prohibitive electromagnetic interference to support the G-6 (S-6) led joint spectrum interference resolution program.
- Participates in the CEMA working group to deconflict EMS requirements.
- Provides advice and assistance in the planning and execution of EW operations.

*Note. The JRFL is a concise list of restricted frequencies and networks categorized as taboo, protected, and guarded.*

## E. Battalion Electronic Warfare Personnel

Battalions have an EW representative responsible for planning and integrating EW capabilities. The EW representative coordinates with the S-2, S-6 staff, fire support officer, the joint terminal attack controller(JTAC), and other staff sections when assigned. In support of a battalion mission, the battalion EW representative requests effects that require coordination with the brigade CEMA section. Battalion EW representatives' duties and responsibilities include—

- Advising the commander on the employment of EW resources.
- Integrating EW during the military decision-making process (MDMP).
- Recommending and implementing EP activities in close coordination with the S-6.
- Managing the maintenance and employment of EW equipment.

# III. Staff Members and Electronic Warfare

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 2-4 to 2-6.

The staff contributes to EW by providing unique products and guidance to the CEWO during all phases of an operation. The same staff members participate in the CEMA working group as necessary.

## G-2 (S-2) Staff

The G-2 (S-2) staff advises the commander and staff on intelligence aspects of EW operations. The G-2 (S-2) staff—

- Provides threat characteristics to support programming of unit EW systems.
- Maintains appropriate threat EW data.
- Maintains the signals intelligence (SIGINT) priorities of collection and informs the staff for situational awareness.
- Ensures electronic threat characteristics requirements are a part of the information collection plan.
- Determines enemy organizations' network structures, disposition, capabilities, limitations, vulnerabilities, and intentions through collection, analysis, reporting, and dissemination.
- Determines enemy EW vulnerabilities and high-value targets.
- Provides intelligence support to targeting operations.
- Assesses the effects of friendly EW activities on the enemy.
- Conducts intelligence gain or loss analysis for EW targets with intelligence value.
- Helps prepare the intelligence-related portion of the EW running estimate.
- Recommends guarded frequencies to the G-6 (S-6) staff for the JRFL.
- Provides updates to the electronic threat characteristics.
- Participates in the CEMA working group to synchronize information collection with EW requirements and deconflict planned EW activities.
- Deconflicts ES and SIGINT operations with the CEMA section.

## G-3 (S-3) Staff

The G-3 (S-3) staff is responsible for the overall planning, coordination, and supervision of EW activities. The G-3 (S-3) staff—

- Plans for and incorporates EW into operation plans and orders, in particular within the fire support plan and the information operations plan (in joint operations).
- Tasks EW activities to assigned and attached units.
- Exercises control over EW, including electromagnetic deception plans.
- Directs EP measures based on recommendations from the G-6 (S-6) staff, the CEWO, and the CEMA working group.
- Coordinates EW training requirements.
- Issues EW support tasks within the information collection plan. These tasks are according to the collection plan and the requirements tools developed by the G-2 (S-2) staff and the requirements manager.
- Ensures, through the CEMA working group, that EW activities support the overall plan.
- Integrates EA within the targeting process.

## G-6 (S-6) Staff

The network defense technician, network management technician, information services technician, spectrum manager, and information security manager participate in planning EW. The G-6 (S-6) staff—

- Assists the CEWO with the preparation of the EP policy.
- Reports enemy EA activity detected by friendly communications and electronics elements to the CEMA working group for counteraction.
- Assists the unit CEWO with resolving EW systems maintenance.
- Identifies and deconflicts electromagnetic interference (EMI).
- Issues the signal operating instructions (SOI).
- Ensures network connectivity for all EW computer systems.
- Provides EMS resources to the unit or task force (refer to ATP 6-02.70).
- Coordinates for EMS usage with higher echelon G-6 (S-6), communications system directorate of a joint staff, and applicable host-nation and international agencies as necessary.
- Prepares the restricted frequency list and issuance of emissions control guidance.
- Coordinates frequency allotment, assignment, and use.
- Supports the CEMA working group by assisting in the development of electromagnetic deception plans and activities that include EMS resources.
- Coordinates with higher echelon spectrum managers for EMS interference resolution.
- Assists the CEWO in issuing guidance to the unit, including subordinate elements, regarding deconfliction and resolution of interference problems and processes involving EW systems.
- Participates in the CEMA working group to deconflict friendly EMS requirements with EW activities and information collection efforts.
- Supports all subordinate unit software updates and communications security (COMSEC) requirements.
- Compiles and distributes the JRFL (Spectrum Manager).
- Assists the EW section with computer maintenance and troubleshooting.

## Information Operations Officer

The information operations officer is responsible for all information operations. To enable information operations, the CEMA section undertakes deliberate actions designed to gain and maintain advantages in the information environment. Typically, but not solely, these actions occur through cyberspace operations and EW. The information operations officer—

- Ensures synchronization and deconfliction with other information operations.
- Considers second- and third-order effects of EW on information operations and proactively plans to enhance intended effects.

## Staff Judge Advocate or Representative

The SJA is responsible for all legal advice. The SJA or representative reviews all EW operations to ensure they comply with existing DOD directives and instructions, rules of engagement (ROE), and applicable domestic and international laws, including the law of war. The SJA may also obtain any necessary authorities that are lacking.

- Establishing battalion EW SOP.
- Submitting EW requests and concept of operations to the brigade CEMA section.
- Coordinating with airborne EW assets to provide the aircraft situational awareness of a ground unit's operational environment including actions on the desired target.
- Establishing and enforcing counter radio-controlled improvised explosive device electronic warfare (CREW) employment. For more information about CREW devices, see paragraph 6-56.
- Conducting all EW related training to battalion and company personnel.
- Managing battalion and company EW resource reprogramming activities more information on reprogramming activities is in chapter 3.
- Conducting operational checks and inspections of EW equipment programs.

## **F. Company Counter Radio-Controlled Improvised Explosive Device Electronic warfare Specialists**

Company CREW specialists, operate, maintain, reprogram, and reconfigure CREW devices for the unit. Commanders rely on CREW specialists to manage the devices within the company. CREW specialists—

- Advise the company commander on the employment of CREW and EW resources.
- Train and assist operators in the use and maintenance of CREW equipment
- Perform pre-combat checks and pre-combat inspections for EW equipment.
- Ensure CREW systems are operational and report deficiencies.

## **G. Electronic Warfare Control Authority**

In some instances, EW personnel in an Army headquarters serve as the EW control authority. The EW control authority establishes guidance for EA on behalf of the joint force commander. If designated as the electronic warfare control authority the senior EW staff officer has the following responsibilities—

- Approve, disapprove, and modify EA requests from within the organization and subordinate units.
- Integrate and synchronizing EA activities.
- Maintain a log containing all approved jamming activity.
- Participate in the development of and ensuring compliance with the JRFL and all other EMS use plans.
- Maintain situational awareness of EA capable systems in the area of operations.
- Deconflict EA and ES, in coordination with the G-2 (S-2), to make recommendations to the combatant commander on intelligence gain or loss.
- Coordinate EA requirements with joint force components.
- Investigate unauthorized EA events and implement corrective measures.
- Approve or deny cease jamming requests.

*Note. Joint organizations designate EW professionals as an electronic warfare control authority as needed. For more information about EW control authority, refer to JP 3-13.1.*

# III. EW Preparation & Execution

*Ref: ATP 3-12.3, Electronic Warfare Techniques (Jul '19), chap. 4.*

Preparation, execution, and assessment are interdependent parts of electronic warfare. This chapter discusses the techniques and resources to prepare, execute and assess electronic warfare effectively. This chapter provides electromagnetic spectrum resource coordination procedures and techniques to mitigate electromagnetic interference.

*See pp. 4-15 to 4-28 for discussion of electronic warfare planning.*

## I. Electronic Warfare Preparation

Peer threats continue to mature their command and control and EW capabilities. To overcome the adversary, units prepare for the contest to dominate the EMS. Preparation begins before arrival on the battlefield and continues through redeployment.

The EW professionals gain proficiencies in EW activities from a combination of military education, doctrinal references, and experience. EW preparation ensures timely support for the commander's scheme of maneuver. Preparation consists of activities that units perform to improve their ability to execute a mission. Preparation for EW includes—

- EW training that includes actual and simulated resources and environments.
- Maintenance activities to ensure that EW equipment is clean and serviceable.
- Practicing the MDMP with other members of the staff. Practicing MDMP fosters teamwork and establishes expectations regarding what the CEWO provides to, and receives from, the staff.
- Rehearsals that include integration of SIGINT & EW resources and capabilities.
- Planning, initiating, and reporting movement of EW resources.
- Coordinating route clearance and escort requirements to mitigate risk and prevent delays during a maneuver.

During preparation, the CEMA section—

- Updates the EW running estimate in coordination with the SIGINT running estimate.
- Requests changes or exceptions to the JRFL and SOI through the G-2 (S-2) and G-6 (S-6) staff.
- Completes risk assessments and develops a risk mitigation strategy.
- Leads the CEMA working group.
- Develops and rehearses battle drills and staff processes including—
- Staffing the EARF and measuring the effectiveness of EW activities.
- Developing EW ground and airborne control authority procedures.
- Integrating information collection activities [G-2 (S-2)] staff.
- Coordinating for external maintenance and reprogramming support for EW assets.
- Initiating EP procedures to counter EMI and enemy jamming actions.
- Developing SOPs.
- Establishing reporting procedures.
- Executes pre-combat checks and inspections of EW assets.



## II. Integration of Electronic Warfare and Signals Intelligence

Integrating EW and SIGINT is a force multiplier for unified land operations. EW and SIGINT have similar capabilities that are mutually beneficial. Integrated EW and SIGINT assets present an efficient, holistic approach that reduces duplication of effort, enables additional information collection, and provides flexibility in the employment of EW and SIGINT resources. EW and SIGINT teams collaboratively use DF techniques to locate transmitters, achieving a higher level of fidelity on the location of emitters. Integration techniques take advantage of similar capabilities and the placement of EW and SIGINT resources to increase operational flexibility, such as co-locating capabilities. SIGINT teams can exploit enemy communications characteristics such as verbal content of a transmission and positively identify an emitter as an approved target. The SIGINT teams can inform the EW team for immediate target engagement.

### A. Distinctions Between Electronic Warfare and Signals Intelligence

Though EW and SIGINT are similar, there are important distinctions between them. Legal considerations distinguish EW and SIGINT activities, and the authorization for each to support operations, that if not observed, can complicate and delay the execution of electronic warfare effects and SIGINT operations. Commanders and planners should collaborate closely with the SIGINT enterprise and legal authorities to ensure compliance with SIGINT policy when planning electronic warfare.

### B. Sensing Activity Distinctions

Commanders have the option to employ SIGINT sensors to support ES activities. The task and purpose are the main factors to decide to use SIGINT or ES capabilities. SIGINT sensors perform ES activities when used to provide immediate threat information including threat warning, avoidance, targeting, and jamming (refer to CJCSI 3320.01D). However, when the SIGINT sensor intercepts, identifies, and locates or localizes sources of intentional and unintentional radiated electromagnetic energy for intelligence purposes, it is no longer supporting an ES task but is conducting a SIGINT mission to satisfy intelligence requirements. These distinctions are identified when answering questions—

- Who tasks or controls the SIGINT sensors?
- What are the sensors tasked to provide?
- What is the purpose of the task driving the employment of the sensors?

ES and SIGINT employ the same or similar capabilities. ES includes 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 3-13.1).

Units retain some data from ES to support immediate threat recognition, targeting, and planning of future operations. Units transfer select data from ES activities to the United States SIGINT System for the production of foreign intelligence. Foreign intelligence is information that relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons (JP 2-0). The CEWO and the G-2(S-2) staff develop a structured procedure within each echelon to facilitate information exchange. Units rehearse this procedure during exercises and pre-deployment planning.

# Deconflicting the Electromagnetic Spectrum

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 4-1 to 4-2.

Deconflicting the EMS requires an understanding of the SOI, JRFL and mission requirements. The CEWO considers the distance, location and the purpose of equipment that is reliant on friendly or restricted frequencies and recommends exceptions to the SOI or JRFL. The SOI contains call signs, call words, frequency assignments, signs, and countersigns for friendly forces.

*For more information regarding the SOI and JRFL, refer to ATP 6-02.70.*

Frequency deconfliction is a systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management (JP 3-13.1).

Mission requirements may drive modifications to the SOI and JRFL. Modifications require staffing and approval through the G-2 (S-2) and G-6 (S-6) staff. For SOI and JRFL deconfliction, the CEWO considers the following—

- The purpose of the frequency.
- Waveform characteristics.
- Location and time of use.

*Note. When EW activities conflict with the SOI or JRFL, the commander decides which has priority.*

Due to security concerns, frequencies employed in intelligence roles may not be included in the SOI. The CEWO maintains awareness of the frequencies used in support of SIGINT activities through coordination with the G-2 (S-2) staff.

## Electromagnetic Spectrum Resources

The authorization to use EMS resources is not always available. The G-6 (S-6) section spectrum manager uses the EMS certification process to gain the use of previously unallocated EMS resources, which requires completing a standard frequency action format.

Host nations have EMS usage plans that assist in the management of frequencies. The spectrum manager assigned to the G-6 (S-6) assists the CEMA section in frequency use authorization for EW activities. The G-6 (S-6) spectrum manager requests frequency resources through an online database. The online database enables managers to determine the historical EMS supportability of like systems. The hyperlink to the DD Form 1494, Application for Equipment Frequency Allocation, to request frequencies is in the references section of this publication.

*See chap. 5, Spectrum Management Operations.*

### III. Electronic Warfare Execution

*Ref: ATP 3-12.3, Electronic Warfare Techniques (Jul '19), pp. 3-12 to 3-13.*

The CEWO addresses targets and employs EW assets in support of an operation. Targeting requires continuous involvement from the CEWO. After planning, the CEWO participates in the targeting board and assesses the effects using measures of effectiveness. During execution the CEWO—

- Prosecutes approved EW targets in support of the operation.
- Evaluates the effectiveness of EW.
- Maintains situational understanding of EW activities and associated effects.
- Oversees the movement and placement of EW assets in support of operational requirements.
- Continues to identify and assess risk.
- Receives information from EW assets and disseminates to the staff:
- Detection and location of targeted and potential enemy emitters, including enemy EW assets.
- Indicators and warnings of enemy activity from EW.
- Maintains direct liaison with the fires cell, G-2 (S-2) and G-6 (S-6) staff to ensure integration and deconfliction of EW activities.
- Coordinates and manages EW missions tasked to subordinate units and requests for nonorganic EW support.
- Continues to assist the targeting working group in target development and to recommend targets for attack and reattack.
- Anticipates EW equipment outages and initiates the capability replacement plan.
- Validates and disseminates cease-jamming requests.
- Coordinates and expedites EMI reports with the G-2 (S-2) and G-6 (S-6) staff for deconfliction.
- Serves as the EW controlling authority when designated.

The CEWO portrays radio wave propagation and EW effects using modeling and simulation techniques with software.

#### Special Considerations During Execution

EMS resources are congested and contested with friendly and enemy use. EMS resource availability also shifts during an operation. The CEWO updates any changes within the EME and puts them into the common operational picture. During execution, EW planners continually consider—

- The Electromagnetic Order of Battle (EOB) (*See p. 5-15.*)
- The signal operating instructions (SOI)
- The Joint Restricted Frequency List (JRFL) (*See p. 4-22*)
- Anticipated or reported Electromagnetic Interference (*See pp. 3-10 & 3-31.*)

# IV(a). Electronic Attack Techniques

*Ref: ATP 3-12.3, Electronic Warfare Techniques (Jul '19), chap. 6. See also pp. 3-3 to 3-5.*

This section discusses the techniques for conducting electronic attack and describes their characteristics. Electronic attack enables the commander to dominate the electromagnetic and supports the scheme of maneuver during Army operations.

## I. Planning Electronic Attack

Commanders use EA to affect threat communications and noncommunications capabilities and for defense. EA is a single action or supplements other lethal or nonlethal attacks. Dynamics in an operational environment require the CEWO to employ different EA techniques based on operational variables. EA techniques include countermeasures and electromagnetic deception. Army operations employ offensive and defensive EA such as—

- Jamming adversary radar or command and control systems.
- Using antiradiation missiles to suppress adversary air defenses.
- Using electronic deception to confuse adversary surveillance and reconnaissance systems.
- Employing self-propelled, towed, or stationary decoys.
- Using self-protection and force protection measures such as use of expendables (e.g., flares and active decoys)
- Employing directed energy or infrared countermeasures systems.

EA includes both offensive and defensive activities. Offensive EA disrupts or destroys threat capability. Defensive EA protects friendly personnel and equipment. When planning EA, the CEMA section, in conjunction with the staff consider—

- Interference of friendly communications.
- Intelligence gain or loss.
- EMS use by locals and non-hostile parties.
- The persistence of effects.
- Electronic signatures.

EA depends on ES and SIGINT to provide targeting information and battle damage assessment. Throughout the MDMP and the targeting process, the CEWO coordinates and deconflicts spectrum requirements with the CEMA working group.

*Refer to JP 3-13.1 for more information about EA and defensive EA planning.*

## A. Electronic Attack Effects

EA denies the enemy or adversary the ability to use the EMS, use equipment, or affects personnel and their decision making or courses of action. The effects that EA creates include denying, destroying, degrading, deceiving, delaying, diverting, neutralizing, or suppressing enemy or adversary EMS capabilities. These effects are mutually exclusive, and these terms are common when describing the desired effects. There may be other terms appropriate to describe desired effects other than those listed. For more information on effects, refer to JP 3-60.

The different EA systems have varying capabilities. The EW personnel planning and employing the variety of systems consider each of the system-specific parameters, the environment, and mission requirements. Each system has specific capabilities and may require ingenuity during planning to ensure mission success.

## B. Electronic Attack (EA) Considerations

*Ref: ATP 3-12.3, Electronic Warfare Techniques (Jul '19), pp. 6-2 to 6-4.*

The CEMA working group plans and rehearses EMS deconfliction procedures. When EA conflicts with the G-2 (S-2) information collection efforts, the commander decides which has priority or the G-3(S-3) decides based on commander's guidance.

The potential for threat intelligence collection also affects EA planning. A well-equipped adversary can detect EA by employing ES techniques to gain intelligence on U.S. force locations and intentions. To develop an understanding of the adversary's intelligence collection capability, the CEWO and the G-2 (S-2) staff develop the enemy EOB. CEWOs protect EA assets through EP and risk mitigation techniques to counter threat ES and EA. For more information about EP, see chapter 7.

A red team provides an independent capability to explore alternatives in plans and operations in the context of an operational environment and from the perspective of enemies, adversaries, and others (JP 2-0). In conjunction with the red team, the CEWO and the G-2 (S-2) staff determine what intelligence the adversary can gain.

### Threat Electronic Warfare Persistence

Aside from antiradiation missiles, the effects of jamming are less persistent than effects achieved by lethal means. The effects of jamming persist as long as the jammer itself is emitting and is in range to affect the targeted receiver. These effects last a matter of seconds or minutes, which makes the timing of such missions critical. Timing is important when units use jamming in direct support of aviation or ground platforms. For example, in a mission that supports suppression of enemy air defense, the time on target and duration of the jamming must account for the speed of attack of the aviation platform. They must also account for the potential reaction time of threat air defensive countermeasures. Because jamming may cause the threat to take unexpected actions or use other means of communications to avoid the intended effect, the CEWO uses ES techniques to sense and validate the persistence of known threat transmissions.

### Electronic Attack to Destroy

An electromagnetic pulse creates a permanent effect and destroys equipment rendering it useless until the threat repairs or reconstitutes the capability. An electromagnetic pulse is the electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges (JP 3-13.1). Units at echelons theater army and below seeking to destroy a target using an electronic pulse rely on strategic level decisions and support to achieve this effect.

### Countermeasures

The Army uses countermeasure techniques to mitigate threat EW sensing and attack activities. Countermeasures are that form of military science that, by the employment of devices and techniques, by design impairs the operational effectiveness of threat activity (JP 3-13.1). Countermeasures can be active or passive and deployed preemptively or reactively. Countermeasure devices and techniques include flares, chaff, radar jammers, CREW systems, and decoys. Chaff is radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion (JP 3-13.1).

### Electromagnetic Deception

Deception mission techniques include misleading transmissions that present false indications offensively force battle rhythms. Control and coordination are necessary to avoid confusing friendly activities with deception missions. When planning an electromagnetic deception mission, the EW planners consider activities that support the current, friendly operation as well as those that will support the deception mission and perform integration

and deconfliction. EW supports all deception plans, both military deception and tactical deception, using the electromagnetic deception and scaling appropriately for the desired effect. Electromagnetic deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an adversary or to adversary electromagnetic dependent weapons, thereby degrading or neutralizing the enemy's combat capability (JP 3-13.1). Electromagnetic deception can increase or decrease ambiguity affecting the enemy decision maker's understanding. This can prove to an enemy commander the certainty of a course of action or create confusion on their behalf.

The G-3 (S-3) staff plans and supervises deception missions. The information operations officer develops deception plans. Integration of electromagnetic deception with information operations is necessary when conducting deception missions. EW supports information related capabilities and deception plans using electromagnetic deception techniques. The CEWO is responsible for the EW portion of the deception plan.

## Simulative Electromagnetic Deception

Simulative electromagnetic deception attempts to represent friendly notional or actual capabilities to mislead threat forces. Simulative electromagnetic techniques require extensive command and staff collaboration to present a believable deception plan. What the threat detects electronically should be consistent with other sources of intelligence reports. Simulative electromagnetic deception transmissions require close attention. Electromagnetic deception effects are often of short duration. Simulative electromagnetic deception includes the use of systems that give off emissions indicative of a particular organization. A counter-mortar or counter-battery radar is organic to an artillery unit. By turning on that type of radar, you can identify the probable location of an artillery unit. Simulative electromagnetic deception also includes using emitters to imply a type or change of activity by a unit, for example, placing surveillance radars in a typical defensive array, when in fact the intent is to attack.

## Manipulative Electromagnetic Deception

Manipulative electromagnetic deception uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit is going to attack when it is going to withdraw, the unit might transmit false plans and requests for ammunition. CEWO's use manipulative electromagnetic deception to mislead the enemy to misdirect their EA and ES assets, while interfering less with friendly communications. Manipulative electromagnetic deception seeks to eliminate, reveal, or convey misleading indicators of friendly intentions. Success in manipulative electromagnetic deception and simulative electromagnetic deception depends on understanding how friendly transmitters appear to the threat. The EW planners consider what is occurring with the friendly transmitters. Then the EW planners determine how to portray the friendly command's transmission infrastructure (JP 3-13.1).

## Imitative Electromagnetic Deception

Imitative deception mimics threat emissions with the intent to mislead them. Imitative electromagnetic deception, if recognized by the enemy, can compromise SIGINT efforts. Imitative deception normally requires approval from higher echelon commands. An example of imitative electromagnetic deception includes entering the adversary's communication nets by using their call signs and radio procedures and then giving threat commanders instructions to initiate actions, which are to the advantage of friendly forces. Targets for imitative electromagnetic deception include any threat receiver and range from cryptographic systems to plain-language tactical nets. Imitative electromagnetic deception can cause a unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts foster decisions based on false information that, to the enemy, appears to have come from within. Imitative electromagnetic deception can be decisive on the battlefield. However, to be effective, imitative electromagnetic deception requires electronic equipment capable of convincingly duplicating the emissions of enemy equipment (JP 3-13.1).

## II. Preparing Electronic Attack

In preparation for EA, the CEWO gathers target information from ES sensors and the EOB. The information includes the location of the targeted asset, electronic characteristics, and the frequencies in use. Using location, characteristics and frequency, the CEWO determines which assets are best to conduct EA. The CEWO then completes calculations to determine the power required to jam the targeted receiver. The CEWO gives guidance to subordinate units about EA. The guidance includes information that allows the subordinate unit to prepare for the EA. EA guidance includes—

- Target identification.
- Target location.
- Special coordination requirements and procedures.
- Jamming technique.
- Jamming duration.
- Desired effect.
- Battle damage assessment method of delivery and prescribed format.

*Note. The CEWO uses formulas to determine minimum power output requirements used for targeting. Refer to ATP 3-12.3, Appendix A.*

### Electronic Attack Considerations

The selection of EA assets is a significant factor when preparing to conduct EA. EA considerations include—

- Concealment characteristics.
- Power output capability.
- Availability of physical protection.
- Time available for the mission.
- Route clearance and escort requirements to conduct friendly maneuver.
- Augmented security coordination.
- Airspace considerations for airborne EW assets.

*See facing page for discussion of Electronic Attack Requests (EARFs).*

## III. Executing Electronic Attack

The CEWO has multiple options to choose from when executing EA. The CEWO prosecutes EA from air and ground (including fixed and mobile) platforms and monitors the EA activities during the mission. Mobile platforms consist of vehicular mounted and dismounted configurations. Units conduct EA using the chosen jamming technique and report the results of the jamming efforts to the CEWO.

### Close Air Support (CAS)

Close air support (CAS) delivers EA using a variety of air platforms. There are two types of CAS requests: preplanned and immediate. The CEWO reviews the air tasking order (ATO) calendar when resourcing EA requirements. When CAS is available, the CEWO submits a request to use CAS for the EA mission.

The air support operations center provides the ATO calendar, which has detailed information on aircraft, crews, and missions. Preplanned CAS requests occur during planning. The ATO calendar is broken down into 24-hour duty cycles. The specific theater or joint operations area supporting joint air operations command and control center will establish cut-off times to receive preplanned air support requests for inclusion in the ATO. Immediate air support requests arise from situations that develop outside the planning stages of the joint air tasking cycle. It is important to understand that air assets available to satisfy immediate air support requests already exist in the published ATO.

*For more information about CAS and the ATO calendar, refer to JP 3-09.3.*



# Electronic Attack Requests (EARFs)

*Ref: ATP 3-12.3, Electronic Warfare Techniques (Jul '19), pp. 6-4 to 6-5. Refer to ATP 3-09.32 and ATP 3-12.3, app D for more information. See also pp. 4-27 to 4-28 (EARF).*

The objective of EA is to disrupt or degrade the threat's ability to receive electromagnetic signals radiating from their transmitters, or process signals from other sources, such as friendly transmissions, with confidence. CEWOs integrate EA into the tactical plan by coordinating with the targeting board and the CEMA working group. The targeting list is an output from the targeting board and specifies the targets and times of attack regardless of the method used. When preparing for EA, the CEWO considers—

- The commander's intent.
- The ROEs.
- The location and identity of the targeted receiver and associated transmitter.
- The electronic threat characteristics of the targeted receiver & associated transmitter.
- The target engagement calculations.
- The associated risk when targeting with EA.

The CEWO makes coordination with the staff to plan EA. The G-2 (S-2) staff provides electronic threat characteristics to aid in the development of targets. The electronic threat characteristics include the technical characteristics of the target. The CEWO maintains electronic threat characteristics for future targeting efforts. Threat characteristics regarding targets include—

- Threat's unit or organization.
- Frequencies in use.
- Call signs.
- Location.
- Power of transmitters.
- Bandwidth.
- Equipment nomenclature.
- Modulation type.
- Multiplex capability.
- Pulse duration.
- Pulse repetition frequency.
- Antenna type.
- Antenna height.
- Antenna orientation.
- Antenna gain.

The CEWO determines the minimum power output required to attack the target receivers. Excessive EA power makes it easier for the threat to locate and attack the friendly EA asset. Distances between the threat transmitter and receiver and the friendly EA asset are critical considerations for EA asset placement.

Terrain is a factor because LOS is necessary between the EA asset and the location of the targeted receiver. The adversary uses terrain to mask transmitted signals from friendly detection and attack. Other terrain considerations include—

- Urban infrastructure.
- Bodies of water.
- Soil composition.
- Vegetation density.

# A. Airborne Electronic Attack

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 6-6 to 6-7.

Airborne EA delivers jamming from rotary, fixed-wing and unmanned aircraft systems. Although some of these platforms are organic to the Army, much of the airborne EA capability resides in other Services. Requesting airborne EA often requires coordination with joint forces. Effective airborne EA requires integrating procedures and communications between the supported unit and the airborne EA asset owner. The EARF includes the prescribed communications method.

Communications between the aircrew, CEWO, and JTAC throughout the mission is beneficial for maintaining situational understanding and for retasking an asset. Best practices include active communications between the CEWO and the aircraft that is delivering the EA.

When the CEWO cannot communicate with the aircrew or the JTAC, the supporting aircraft continues with the airborne EA mission specified in the EARF. A technique is to note in the EARF regarding what to do in the event of a communication failure (FM 3-12).

## Canceling and Retasking Airborne Electronic Attack

Changes within an operational environment and EA missions make it necessary for reprioritization of assets. Air platforms are in demand for other purposes such as surveillance supporting intelligence missions or signal missions. The CEWO can request dynamic retasking of airborne EA assets and requests retasking with the JTAC and the air operations center.

## Joint Tactical Attack Controller

The JTAC conducts air and ground coordination. The JTAC initiates requests and maintains communications with the designated airborne EA point of contact for the duration of the mission.

## Air Operations Center

The air operations center, which can be joint or allied depending on the task organization, coordinates all assigned aerospace forces. The air operations center conducts the following activities—

- Coordinates and approves airspace.
- Coordinates aerial refueling.
- Makes ATO changes.
- Issues retasking instructions.

## Airborne Electronic Attack Cancellations at the Battalion and Brigade

Sometimes it is necessary to cancel airborne EA missions. CEWOs communicate cancellations to the asset owner and requestor points of contact. Reporting cancellations ensures the most efficient use of EA assets and availability for other missions.

## Advanced Cancellation of Preplanned Mission

When a CEWO cancels an airborne EA mission more than six hours before a preplanned mission is a routine task. The requestor includes the reason for cancellation. The CEWO immediately communicates a cancellation of a mission to release the airborne EA asset for other missions. The CEWO also notifies the fire support officer and the air liaison officer. Cancellations made during operations include direct voice communications when possible to ensure someone is available and ready to process the cancellation.

## Short Notice Cancellation of Preplanned Mission

Short notice airborne EA cancellations are cancellations that occur less than six hours before a preplanned mission. Short-term cancellations require immediate action to avoid mission launch and the unnecessary employment of an asset. The CEWO informs the designated point of contact that a cancellation is coming by the most expeditious means available. Following the initial notification, the CEWO sends the official cancellation joint tactical air strike request (JTASR) to the appropriate point of contact as soon as possible. Since the cancellation may require communications that bypass normal chain of command relationships, CEWOs include the process in the written unit SOPs and battle drills.

## Immediate Cancellation of Preplanned Mission

CEWOs use this technique for canceling missions within one-hour of the expected execution time. CEWOs use the fastest communication means possible, such as Internet relay chat or voice communications, to distribute the necessary cancellation information. Immediately following an immediate cancellation, CEWOs contact the prescribed point of contact and provide an official cancellation using the points of contact on the JTASR and EARF to ensure units receive information promptly. Effective units include this process in the unit SOP and battle drills.

## Dynamic Retasking

The staff makes every effort to provide immediate EA in response to an urgent request, including the allocation of available airborne EA assets. The retasking of airborne EA assets fulfills requests for on-demand requirements.

The process for retasking airborne EA platforms varies depending on joint command and control and Army mission command arrangements, task organization, force disposition, and unit boundaries. The requesting unit submits a request to their supporting EW representative. The retasking format is available in ATP 3-09.32.

If the requesting unit previously submitted a JTASR for EA support, the CEWO modifies the existing JTASR with a numbered change. Some units make the change using red for easier identification. If the requesting unit has not submitted a JTASR for the mission, the CEWO creates a new JTASR. The CEWO provides status updates to the requesting unit. Effective units address the knowledge management processes for maintaining updated JTASRs in their SOPs and battle drills. Due to the dynamic nature of an urgent requirement, there is no way to calculate the amount of time needed for coordinating the airborne EA. The CEWO or JTAC notifies the appropriate EW representative and air support operations center when it is apparent that the duration of EA will exceed the initially anticipated time. The air support operations center notifies the airborne EA asset and coordinates any additional fuel requirements or determines the need to re-task another airborne EA asset. The air support operations center then informs the CEWO and JTAC of what support to expect. The JTAC or CEWO contacts the air support operations center to release airborne EA assets upon mission completion or cancellation.

## Jamming Techniques

CEWOs use jamming techniques to disrupt the threat's ability to effectively receive or process electromagnetic signals by overcoming the threat receiver with higher power transmissions. Successful jamming of receivers requires an understanding of available jamming techniques. CEWOs consider which technique is appropriate to support the commander's intent. Jamming techniques include—

- Electromagnetic jamming.
- Electromagnetic intrusion.
- Electromagnetic pulse.
- Electronic probing.

## B. Defensive Electronic Attack

Defensive EA degrades the threat's ability to employ weapons that use electromagnetic activated triggers. Defensive EA protects friendly personnel and equipment. Counter radio-controlled improvised explosive device (RCIED) systems implement this EA technique.

Defensive EA uses the EMS to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and other protection measures such as the use of expendables (flares and active decoys), jammers, towed decoys, directed-energy infrared countermeasures, and counter RCIED systems(FM 3-12).

### Counter Radio-Controlled Improvised Device (CREW)

A common form of defensive electronic attack is counter radio-controlled improvised explosive device electronic warfare (CREW). CREW systems jam threat radio frequencies to prevent RCIEDs from receiving a triggering signal, thus stopping the RCIED from detonating. Units program CREW systems with threat-specific loadsets based on various sources of intelligence, including the technical exploitation of recovered RCIEDs. The loadset is what the device uses to determine its operational frequency range, change rate, and other attributes of the system. The loadset is essentially what programs the system to operate under predetermined parameters based on an operational environment. The Army employs mounted, dismounted, and fixed CREW systems as electronic countermeasures to RCIED attacks.

### Cyber Electronic Warfare Officer Role

The CEWO is the commander's subject matter expert on CREW. The CEWO plans the inclusion of CREW in support of operations, establishes maintenance procedures and ensures reprogramming and configuration of CREW devices.

## IV. Electronic Attack Techniques in Large Scale Combat Operations

Peer and near-peer adversaries rely on the EMS for command and control, sensing and targeting, and EW. Units require EA capabilities during large-scale combat operations to counter adversary communications and noncommunications emitters.

When jamming threat communications, the CEWO aligns EW capabilities with targets. The EA does not jam every threat communication. The EA is only disrupting the communication between the enemy battalion and enemy company. The close proximity and transmit power of the radios of the enemy tanks in a company formation allows them to maintain uninterrupted communications. The battalion transmissions to the company have a greater distance to travel and weaker signal at the receiving antenna leaving the communications vulnerable to EA.

Adversaries employ multiple sensors and noncommunications emitters, such as radars, to detect and locate friendly forces during large-scale combat operations. The CEWO uses EW activities, such as electromagnetic deception, combined with EW techniques to disrupt the adversary's ability to target friendly forces. The CEWO also disrupts adversary SIGINT and ES sensors to prevent detection, locating, and exploitation of friendly transmitters.

The CEWO understands that during large-scale combat operations, the threat has EW capabilities that can negatively affect friendly operations. The threat conducts EA to degrade communications and achieve a tactical advantage during operations. Units must incorporate EP techniques to counter threat EA activities.

# IV(b). Electronic Protection Techniques

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), chap. 7.

The greatest threat to mission command information systems at the tactical level is the enemy's use of electronic warfare assets to geolocate and jam friendly communications. This chapter discusses electronic protection and the techniques used to overcome electromagnetic interference. Successful electronic protection requires planning and execution by all members of the unit.

EP is the sum of technology, equipment, and techniques used to counter threat EW activities. EP is not force protection or self-protection. EP is an EMS-dependent system's use of electromagnetic energy or physical properties to preserve itself from direct or environmental effects of friendly and adversary EW, thereby allowing the system to continue operating (JP 3-13.1).

See also pp. 3-6 to 3-7.

## Commander's Electronic Protection Responsibilities

EP is a command responsibility. Commanders ensure that all Soldiers in their units' train to apply EP techniques. Commanders rely on the staff to mitigate electronic vulnerabilities. The staff continuously measures the effectiveness of the applied EP techniques. Commanders' EP responsibilities are—

- Read after action reviews and reports about threat jamming or deception efforts and assess the effectiveness of EP.
- Ensure the staff reports and analyzes EMI, deception, or jamming.
- Analyze the impact of threat efforts to affect friendly communications.
- Ensure the unit incorporates appropriate EP techniques such as—
- Changing network call signs and frequencies in accordance with the SOI.
- Using approved COMSEC devices.
- Loading and using prescribed encryption keys.
- Using planned authentication procedures.
- Controlling emissions.

## I. Planning Electronic Protection

Electronic protection uses techniques such as limiting transmissions and using natural or manmade objects to mask radiated energy from traveling to undesirable destinations. Electronic protection is essential to prevent the adversary from learning behavior and intentions within the EMS.

The CEWO considers friendly communications asset characteristics, their priorities for protection and their purpose of employment when planning EP. Additionally, the CEWO considers adversarial EW and SIGINT capabilities and their use against friendly systems. The G-6 (S-6) is the primary source for gaining the characteristics of friendly communications resources while the G-2 (S-2) is the CEWO's primary resource to gain electronic threat characteristics.

See following page for an overview of EP considerations.

# Electronic Protection Considerations

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 7-1 to 7-2.

EP includes physical security, COMSEC measures, system technical capabilities, such as frequency hopping, shielding of electronics, electromagnetic spectrum management, and emission control procedures. EP is an EMS-dependent system's use of electromagnetic energy and/or physical properties to preserve itself from direct or environmental effects of friendly and adversary EW, thereby allowing the system to continue operating (JP 3-13.1). The CEWO considers the following for EP—

- Vulnerability analysis and assessment of friendly communications assets.
- EP monitoring techniques and feedback procedures.
- EP effects on friendly capabilities.

## Vulnerability Analysis and Assessment

Vulnerability analysis and assessment form the basis for developing EP plans. The CEWO reviews the unit EP techniques and procedures to determine weaknesses and develops plans for improvement. The G-6 (S-6), United States Cyber Command, and the Defense Information Systems Agency provide a variety of cybersecurity services, including vulnerability analysis and assessments.

The National Security Agency monitors COMSEC and provides security posture feedback to units. Its programs focus on telecommunications systems using wire and electronic communications. Their programs can support and remediate the command's COMSEC procedures.

## Electronic Protection Effects on Friendly Capabilities

The CEWO and the G-6 (S-6) consider effects on friendly communications when developing an EP plan. A plan that maximizes EP can overly restrict the friendly use of communications assets. The CEWO maintains a balance regarding the unit's ability to communicate with the planned level of EP. EP effects on friendly communications are included in the CEWO's risk assessment. The CEWO and G-6 (S-6) present the risk assessment to the commander during the MDMP. The commander decides what level of risk is acceptable. For EP planning, the CEWO and G-6 (S-6) consider the following—

- Electromagnetic hardening.
- Electronic masking.
- Emission control.
- Electromagnetic spectrum management.
- Wartime reserve modes.
- Electromagnetic compatibility.

# II. Electromagnetic Interference (EMI)

EMI prevents successful transmissions. Units must recognize and mitigate EMI to create the conditions required to use the EMS to communicate. Electromagnetic interference is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment (JP 3-13.1).

## A. Recognizing Electromagnetic Jamming

Radio operations require that radio operators can recognize electromagnetic jamming. Recognizing electromagnetic jamming is not always an easy task; the cause of EMI can be internal and external. If the EMI remains after grounding or disconnecting the antenna, the disturbance is most likely internal and caused by a malfunction of the radio. Contact maintenance personnel for repairs or replace the faulty equipment. Eliminate or substantially reduce the EMI or suspected jamming by grounding the radio equipment or disconnecting the receiver antenna. If measures to eliminate the radio as the source of the disturbance are unsuccessful, it is most likely external to the radio. Check external EMI further for threat jamming or unintentional EMI.

Sources, other than jamming, cause EMI. Unintentional EMI is caused by—

- Friendly and threat use of the same frequencies.
- Other electronic or electric and electromechanical equipment.
- Atmospheric conditions.
- Malfunction of the radio.
- A combination of any of the above.

Unintentional EMI normally travels a short distance; a search of the immediate area may reveal its source. Moving the receiving antenna short distances may cause noticeable variations in the strength of the interfering signal. Conversely, little or no variation normally indicates threat jamming. Regardless of the source, take appropriate actions to reduce the effect of EMI on friendly communications.

Signal	Description
<b>Random Noise</b>	It is indiscriminate in amplitude and frequency. It is similar to normal background noise. Random noise degrades all types of signals. Operators often mistake it for receiver or atmospheric noise and fail to take appropriate electronic protection actions.
<b>Stepped Tones</b>	Tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Single-channel amplitude modulation or frequency modulation use stepped tones for voice circuits.
<b>Spark</b>	Spark is one of the most effective jamming signals. Spark uses short intensity and high intensity; they repeat at a rapid rate. This signal is effective in disrupting all types of radio communications.
<b>Gulls</b>	Generated by a quick rise and slow fall of a variable radio frequency and are similar to the cry of a seagull. It produces a nuisance effect and is very effective against voice radio communications.
<b>Random Pulse</b>	Pulses of varying amplitude, duration, and rate are generated and transmitted. They disrupt teletypewriter, radar, and all types of data transmission systems.
<b>Wobbler</b>	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.
<b>Recorded Sounds</b>	Any audible sound, especially of a variable nature, distracts radio operators and disrupts communications. Music, screams, applause, whistles, machinery noise, and laughter are examples of recorded sounds.
<b>Preamble Jamming</b>	A broadcasted tone over the operating frequency of secure radio nets resembles the synchronization preamble of the speech security equipment. Preamble jamming results in all radios being locked in the receive mode. It is especially effective when employed against radio networks using speech security devices.

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), table 7-2. Common jamming signals.



## B. Remedial Electronic Protection Techniques

Remedial EP techniques that help reduce the effectiveness of threat jamming efforts are the—

- Identification of threat jamming signals.
- Determination of the EMI as being obvious or subtle jamming.
- Recognition of jamming causing EMI by—
- Determining whether the EMI is internal or external to the radio.
- Determining whether the EMI is deliberate or unintentional.
- Reporting of jamming and other EMI incidents.
- Overcoming of jamming and EMI by adhering to the following techniques—
- Continue to operate.
- Diagnose the root cause of EMI.
- Improve the signal-to-jamming ratio.
- Adjust the receiver settings.
- Increase the transmitter power output.
- Adjust or change the antenna.
- Establish a retransmission station.
- Relocate the antenna.
- Use an alternate route for communications.
- Change the frequencies.
- Acquire another satellite or retransmission station.
- Installation of firmware and update software.
- Use enhancements to tactical radio ancillary communications electronics equipment and COMSEC devices.

## C. Concealment

EP plans include provisions to conceal communications personnel and equipment. Though physical concealment is ineffective in changing the EMS signature, obscuring the physical attributes may prevent positive identification of the equipment as a communications system. Units use camouflage material to cover communications assemblages and their power generators. It is difficult to conceal most communications systems. However, installing antennas as low as possible on the backside of terrain features, and behind manufactured obstacles help conceal communications equipment while still facilitating effective communications.

## D. Threat Electronic Attack on Friendly Command Nodes

Adversaries attack or exploit friendly command nodes that support operations. They have developed and equipment and techniques to contest the friendly use of the EMS. Friendly units use EP measures to counter threat EW and exploitation actions against friendly communications nodes.

Adversary attack on friendly command nodes can disrupt or destroy information, intelligence gathering efforts, and communications that support weapons systems. Threat forces expend considerable resources gathering intelligence about U.S. forces. Goals or effects may include—

- Jam friendly communications.
- Enter friendly radio networks.
- Collect information and intelligence about friendly forces.

## E. Electromagnetic Interference (EMI) Battle Drill

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 7-8 to 7-9.

Some prohibitive EMI has a measurable, operational impact. Units execute battle drills to address prohibitive EMI. An EMI battle drill helps isolate the cause of interference and dispel erroneous assumptions about its cause. For example, knowing that CREW devices are jammers may lead to a hasty assumption that a CREW device impairs the use of combat net radios when operator error or faulty equipment is the cause of the EMI. The uninformed assumption that CREW systems are the problem leads to an unnecessary loss of confidence in EW equipment. Lack of confidence in equipment can lead to reluctance to prosecute EW and can have a negative impact on operations. Proper analysis uses sensors and indicators that identify interfering frequencies, the levels of transmission power and receiver strength.

*Note. Watts express the radio transmission output levels, while decibels (dB) express radio receive signal strength. For more information about decibels, refer to ATP 2-22.6-2.*

7-42. The lowest element or individual experiencing the EMI should report the interference via the Joint Spectrum Interference Resolution Website. If unable to access the website, contact someone to input the information into the website at the earliest convenient time. On a staff, normally the G-6 (S-6) staff submits JSIR reports to resolve interference. When appropriate, the staff disseminates the mitigating steps to subordinate units as lessons learned and best practices to avoid future interference. A well-constructed EMI battle drill, guides units to respond to JSIR reports in a consistent, methodical manner. Table 7-3 provides an example of an EMI troubleshooting battle drill.

Signal	Description
1	Follow equipment troubleshooting (verify frequency, cable and antenna connections, communications security). If EMI continues, then follow remaining steps.
2	Determine start and stop times or duration of EMI.
3	Identify EMI effect (interfering voice, noise, static).
4	Identify other emitters in area of operations.
5	Check adjacent and nearby units for similar problems.
6	Prepare and submit a joint spectrum interference resolution report to S-6.
<b>LEGEND</b>	
EMI	electromagnetic interference
S-6	battalion or brigade signal staff officer

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), table 7-3. *Electromagnetic interference troubleshooting battle drill.*

### III. Staff Electronic Protection Responsibilities

The staff implements the EP plan for the commander. Staff responsibilities are—

- Planning, coordinating, and supporting the execution of EP activities (CEMA working group).
- Advising the commander of threat EMS related capabilities [G-2 (S-2) staff].
- Supervising the CEMA section and include EP scenarios in command post, field training exercises, and evaluates employed EP techniques [G-3 (S-3) staff].
- Work with the CEWO to prepare and conduct the unit EP training program. Ensure there are PACE means of communications to support mission command. Distribute COMSEC. Perform friendly frequency management duties and issues the SOI. Review the JRFL and prepares which includes a restricted frequency list of taboo, protected and guarded frequencies [G-6 (S-6) staff].

*Note. The PACE plan compliments EP as it provides multiple means of communications and designates the order in which an element will move through available communications methods until contact can be established with the desired recipient.*

Preventive EP techniques include all measures taken to avoid threat detection and threat EA. EP seeks to mitigate threat information collection and intelligence gathering efforts. Electronic communications equipment has built-in features used to mitigate threat EA, ES and SIGINT actions. CEWOs advise the use of built-in features and user tactics, techniques, and procedures for countermeasures against threat actions.

### IV. Equipment and Communications Enhancements

Some communications equipment has embedded capabilities used to prevent jamming, locating and listening by threat forces. Operators use the embedded capabilities when supporting operations.

#### Frequency-Hopping Mode

Some peer and near-peer adversaries with advanced EW equipment can jam radios that use frequency-hopping techniques. Single channel transmissions are vulnerable to jamming by unsophisticated transmitters, so units use frequency-hopping mode but remain vulnerable to threat EA and DF efforts. Frequency hopping is useful in mitigating the effects of threat jamming, and in keeping friendly position location data from threat forces.

#### Adaptive Antenna Techniques

Adaptive antenna techniques result in more survivable communications. These techniques typically link with spread spectrum waveforms to combine frequency hopping with pseudo-noise coding. Pseudo-noise coding is a technique to make spread spectrum waveforms and frequency-hopping mode appear to be unintelligible noise to an unintended receiver. Spread spectrum is a form of wireless communication in which the frequency of the transmitted signal varies deliberately. This uses more bandwidth than the signal would have otherwise, making it less susceptible to interference.

#### Frequency Hop Multiplexer (FHMUX)

The frequency hop multiplexer (FHMUX) and vehicular whip antennas that support FHMUX are available for use to enhance very high frequency (VHF) communications. The FHMUX is an antenna multiplexer used with single channel ground and airborne radio system in stationary and mobile operations. This FHMUX allows multiple radios to transmit and receive through one VHF antenna while operating in the frequency-hopping mode, single channel mode, or a combination of both. Using one antenna reduces visual and electronic profiles of command posts and reduces emplacement and displacement times.

# IV(c). Electronic Warfare Support Techniques

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), chap. 5.

## I. Planning Electronic Warfare Support

Threat forces use the EMS to give orders, monitor and manage operations, detect aircraft using radar, and conduct DF. Locating threat transmitters aids in the development of situational understanding and assists with targeting. ES uses direction-finding techniques to find threat transmitters. Once located, the commander can direct fires in the form of lethal attack, request offensive cyberspace operations or use EA to gain the desired effects.

See also pp. 3-8 to 3-9.

### A. Electronic Reconnaissance

5-2. Electronic warfare personnel conduct electronic reconnaissance to understand the types of threat emissions. Electronic reconnaissance is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-13.1). The CEWO acquires electronic threat characteristics from the G-2(S-2). The electronic threat characteristics provide technical data including—

- Threat EMS resources in use.
- Antenna orientation and polarization.
- Radio transmit power levels.
- Radio range.

### B. Electronic Warfare Support Considerations

The task and purpose of the mission determine whether a SIGINT or EW asset is appropriate for a given mission. ES assets conduct immediate threat recognition, targeting, future operations planning, and other tactical actions such as threat geolocation for avoidance.

The adversary employs electronics security measures to prevent the detection of emitters. Electronics security is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar (JP 3-13.1). When the adversary employs electronic security measures, the CEWO may require assistance from SIGINT to understand the nature of the emissions.

## II. Preparing Electronic Warfare Support

The CEMA section uses ES assets to scan the EME for transmissions and then illustrates the results in a manner that the commander and staff can understand. Units develop an electromagnetic environment survey using air, ground, and sea platforms. The G-2 (S-2) staff assists the CEMA section by developing and maintaining the electromagnetic environment survey (refer to FM 2-0). The electromagnetic environment survey aids the CEWO to understand the nature, limitations, and sources of EMI in an operational environment and plan the employment of ES equipment. The CEMA section submits requests for information to address information gaps to the G-2 (S-2) staff.

The electromagnetic environment survey provides input, and the CEMA section enters the information into automated tools to maintain a current environment survey.

### III. Executing Electronic Warfare Support

The CEWO and G-2 (S-2) mutually develop the SOPs and battle drills for integration of EW support and SIGINT information collection activities. Integration techniques take advantage of similar equipment capabilities and fuse EW and SIGINT resources to increase flexibility. SIGINT teams pass targeting information to EW teams. The SIGINT DF equipment compliments geolocation efforts and transitions a LOB into a cut or a fix for targeting. Integration facilitates immediate sharing of information and reduces delays in targeting.

#### A. Electromagnetic Environment (EME) Survey

Like weather reports for aircraft pilots, the EME survey informs the CEWO about the activities and conditions of the EME, enabling the CEWO to choose optimal COAs for EW. EME surveys begin with the enemy EOB. The enemy EOB provides the CEWO with an initial overview of threat EMS capabilities derived from IPB. The enemy EOB assists the CEWO in making EW plans that exploit adversary vulnerabilities while preserving friendly capabilities. The enemy EOB is the baseline for the EME survey.

##### Electromagnetic Environment Survey

A unit tasks an airborne EW asset to support suppression of enemy air defense missions. During mission planning, the crew receives the EOB for the area of operations. The airborne EW crew identifies threat emitters they will likely encounter during the mission by priority, and de-conflicts friendly and neutral emitters.

As the airborne EW crew enters the target area of operations, they conduct an EME survey that confirms the presence of friendly, neutral, and threat emitters. Conducting an EME survey allows the crew to prioritize their activities against confirmed threat emitters by only targeting systems that are active.

#### B. Direction Finding (DF)

When conducting DF, the CEWO leverages the arrayed ES assets and coordinates support from the G-2 (S-2) for SIGINT resources to sense transmitters, collect information and triangulate the location of specified emitters of interest. The CEWO provides targeting requirements to the targeting board. Additionally, the CEWO shares the information collected from ES assets during DF activities with the G-2(S-2). The G-2 (S-2) considers information derived from ES when developing intelligence.

DF provides LOBs, cuts, and fixes to locate transmitters. A LOB is a single approximate azimuth from a sensor providing the approximate azimuth to the transmitter. A cut is two approximate azimuths providing the general location of a transmitter by determining where two LOBs intersect. A fix is three or more approximate azimuths providing a location using a triangulation method. A cut or fix may use approximate azimuths from one sensor receiving the signal multiple times from different locations, or from different sensors.

*Refer to ATP 3-12.3, Electronic Warfare Techniques (Jul '19), pp. 5-3 to 5-10 for an overview of and discussion of line of bearing, cuts, fixes, establishing a direction finding baseline, and what causes direction finding errors.*

# IPB Cyberspace Considerations

Ref: ATP 2-01.3, *Intelligence Preparation of the Battlefield* (Mar '19), app. D.

## Intelligence Preparation of the Battlefield (IPB)

Intelligence preparation of the battlefield 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 (ATP 2-01.3). Led by the intelligence officer, the entire staff participates in IPB to develop and sustain an understanding of the enemy, terrain and weather, and civil considerations. IPB helps identify options available to friendly and threat forces.

IPB consists of four steps. Each step is performed or assessed and refined to ensure that IPB products remain complete and relevant:

- Define the Operational Environment
- Describe Environmental Effects on Operations
- Evaluate the Threat
- Determine Threat Courses of Action

IPB begins in planning and continues throughout the operations process. IPB results in intelligence products used to aid in developing friendly COAs and decision points for the commander. Additionally, the conclusions reached and the products created during IPB are critical to planning information collection and targeting.



Refer to BSS6: *The Battle Staff SMARTbook*, 6th Ed., pp. 3-3 to 3-52 for complete discussion of Intelligence preparation of the battlefield from ATP 2-01.3.

\* Refer also to INFO1: *The Information Operations & Capabilities SMARTbook*, pp. 4-17 to 4-34 for related discussion of information environment analysis (IO and intelligence preparation of the battlefield) from ATP 3-13.1.

As an essential part of the information environment, there is a massive global dependence on the cyberspace domain for information exchange. With this dependence and the associated inherent vulnerabilities, the cyberspace domain must be considered during each step of the IPB process:

- **Step 1—define the OE:** Visualize cyberspace components and threats through the three layers of cyberspace.
- **Step 2—describe environmental effects on operations:** Use military aspects of terrain.
- **Step 3—evaluate the threat:** Evaluate threats and HVTs in cyberspace against the warfighting functions by performing critical factors analysis (CFA).
- **Step 4—determine threat COAs:**
  - Consider the threat's historical use of cyberspace and incorporate threat COAs.
  - Determine HVT lists within the cyberspace domain.
  - Assist the S-6 staff to identify friendly networks that require protection.

To gain situational understanding, the following staff sections, in addition to assistance and support from the cyber mission force, provide the G-2/S-2 enough information to develop IPB products that include cyberspace considerations. The G-2/S-2 relies on the—

- G-3/S-3 to task operational assets to report items significant to cyberspace (such as satellite dish locations, cyber cafés, cellular network towers), since the G-3/S-3 is typically aware of maneuver and/or reconnaissance elements moving through specific designated AOs that have the potential to interact with the populace and the ability to visually confirm relevant infrastructure.
- G-6/S-6 for the friendly force network design to determine where the threat can possibly access friendly systems.
- G-9/S-9 to assist in identifying and confirming civil considerations that are pertinent to the cyberspace domain. For example, civil affairs teams may assist in ascertaining existing and planned network infrastructure in the AO, as well as identifying key leaders and landowners to determine their internet presence, activity, or cyber-personas.
- Information operations officer to primarily synchronize and deconflict information-related capabilities employed to support unit operations. With information provided by the intelligence, the information operations officer contributes to IPB by analyzing the information environment and developing the combined information overlay. Working with the intelligence staff, the information operations officer develops products that portray the information infrastructure of the AO and aspects of the information environment that can affect operations. These products include information all audiences and other decision makers, key people, and significant groups in the AO. They also address potential strengths and vulnerabilities of adversaries and other groups. The information operations officer will also assist in identifying how the populace communicates within the logical network layer, such as local government websites, heavily used social media sites, any group or individual blog sites. Additionally, the information operations officer can possibly identify threat TTP for deception and denial of information within the logical layer.
- Cyberspace electromagnetic activities section to provide information on enemy cyber forces' doctrine, tactics, and equipment, and for cyber capabilities for information collection. Cyberspace capabilities cross cue with SIGINT capabilities to provide better situational awareness of threat forces operating in the cyberspace domain.

*Note. Although the intelligence, operations, and signal staff sections are the primary collaborators regarding gaining situational understanding in cyberspace, all staff sections are valuable, to some degree, and should not be disregarded during the staff integration process.*

## Step 1 — Define the Operational Environment

When defining the OE, cyberspace includes information and its communications. Although there are other variables in cyberspace that warrant attention (such as individuals, organizations, and systems), they either process, disseminate, or act on information.

### A. Step 1 Cyberspace Considerations

When defining the OE, consider the three layers of cyberspace—physical network, logical network, and cyber-persona. When evaluating the OE, staff collaboration and reachback assets are essential.



## Physical Network Layer

Depicting the physical network layer within the AO allows the intelligence staff to analyze the physical network layer as it relates to friendly and threat operations. Analysts derive the physical network layer depiction from single-source reporting, all-source intelligence products, cyber mission forces reporting, and other reporting sources. These products assist in developing the physical network layer.

When analyzing the physical network layer, identify—

- Threat C2 systems that traverse the cyberspace domain.
- Critical nodes the threat can use as hop points in the AO and area of influence. Note. Data packets pass through bridges, routers, and gateways as they travel between their sources and destinations. Each time data packets pass to the next network device, a hop occurs.
- Physical network devices in the AO, such as fiber optic cables, internet exchanges, public access points (internet cafés), server farms, and military or government intranets.
- Elements or entities (threat and nonthreat) interested in and possessing the ability to access data and information residing on and moving through the network.
- Physical storage locations with the most critical information and accessibility to that information.
- Critical nodes and entry points the threat is most likely to use to penetrate the network, including mobile tactical communications systems.
- Implemented measures that prevent threat actors from accessing the networks.

## Logical Network Layer

Depicting the threat's logical network layer discloses how and where it conducts cyberspace operations. It is also useful to understand how and where the population exists, socializes, and communicates within the logical network layer. Additionally, network maps often depict the logical network layer in relation to the physical network layer. All-source intelligence analysis can enhance this depiction.

Reporting from many sources can provide information about the logical network layer of threat cyberspace, including but not limited to protocols, internet protocol address blocks, and operating systems. The network's key systems can be assessed using the depiction on the logical network layer.

When analyzing the logical network layer, identify—

- Websites or web pages that influence or have a social impact on the AO.
- Friendly logical network configurations and vulnerabilities and the friendly physical network configurations.
- Current activity baselines on friendly networks, if possible.
- Through which uniform resource locators (known as URLs), internet protocol addresses, and other locations that critical mission data can be accessed on the internet.
- How friendly data is shared and through which software.

## Cyber-Persona Layer

Depicting the threat cyber-persona layer begins with understanding the organizational structure. Assessment of the organizational structure is an all-source intelligence task. Understanding the organizational structure leads to assessing the cyber-personas associated with the organization. These include cyber-personas that represent the organization, subordinate elements, and personnel.

When analyzing the cyber-persona layer, identify—

- Threat presence in and usage of the cyberspace domain.
- Data and information consumers in the AO.
- Hacktivists in the AO, specifically with the intent to disrupt.
- Entities capable of penetrating the networks.
- How local actors interrelate with the physical network (mobile phone or internet café) and logical network (websites or software) layers.

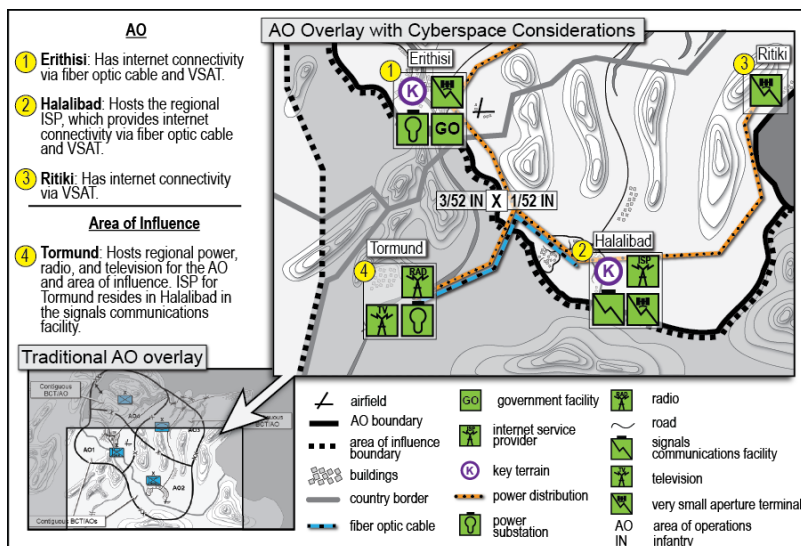
A primary objective when analyzing the cyber-persona layer from an all-source perspective is to identify the physical persons that created and/or used cyber-personas of interest. All-source analysts gain valuable insight by using various tools and techniques, such as link diagrams (refer to ATP 2-33.4) informed by internet and social media usage, linking or associating one or more of the following, both suspected and confirmed, but not limited to cyber-personas, people, websites, internet protocol addresses, organizations or groups, buildings or facilities, and activities.

While on the internet, multiple users can use a single cyber-persona and a single user can use multiple cyber-personas. A user may have multiple cyber-personas for various reasons. This is not necessarily an indicator of illicit activity. However, multiple users using a single cyber-persona may indicate a group's activity or common affiliations.

## B. Cyber-Centric Activities and Outputs for Step 1

The intelligence staff completes the graphic display of significant characteristics and components of cyberspace in relation to the unit's AO and area of influence, as illustrated in figure D-2. If known, it may be beneficial to label those websites frequently visited by the local populace, including Dark websites. Figure D-2 also exhibits the contrasts between a traditional AO overlay and an AO overlay with cyberspace considerations.

*Note. Since cyberspace is a global domain, threats can potentially affect a BCT's battlefield from anywhere in the world. This must be considered when analyzing and establishing the AOI and area of influence.*



Ref: ATP 2-01.3, fig. D-2. Area of operations and area of influence example.

## Step 2 — Describe Environmental Effects on Operations

Although steps 3 and 4 of the IPB process offer a detailed analysis of threats within the OE, the type of threat and their cyberspace capabilities should be defined during step 2. The significance of a cyber force presence should be considered with and weighed against identified variables within the OE.

### A. Step 2 Cyberspace Considerations

*For environmental effects on operations associated with step 2, describe how the following can affect friendly and threat operations:*

- Threats in cyberspace.
- Terrain in cyberspace.
- Weather, light, and illumination data.
- Civil considerations.

### Military Aspects of Terrain

Conduct terrain analysis of the cyberspace domain using traditional methods. Examine the five military aspects of terrain (OAKOC) factors, which can be displayed in a MCOO. Analyzing terrain in cyberspace, as in geographic terrain, can favor either friendly or threat forces. Table D-1 presents the military aspects of terrain with corresponding cyberspace considerations. This allows commanders to understand the terrain's impact, both geographically and in cyberspace, on friendly and threat operations.

<i>Military aspects of terrain (OAKOC factors)</i>	<i>Cyberspace considerations</i>
Observation and fields of fire	Ability to see subnets within networks, intrusion detection systems, password protections, and encryptions used in the area of operations. It is essential to understand what portion of the network can be seen and from where it can be seen. This may include the ability to see using physical surveillance. Additionally, closed networks may prevent observation on friendly and threat networks. Intrusion protection systems may eliminate possible threats across the network.
Avenues of approach	Method of network access, such as an access point, threat intrusion, or path to the physical or logical key terrain, such as switches, routers, servers, and vectors. Mobility corridors can be identified and grouped according to network speed, where slow speeds can cause restricted or severely restricted terrain. The volume of network activity may create additional avenues of approach.
Key terrain	Key terrain can be applied to the physical network, logical network, or cyber-persona layer. Key terrain associated with cyberspace can be considered as a physical node or data that is essential for mission accomplishment. Examples include major lines of communications, key waypoints for observing incoming threats, domain name servers, network operating systems, switches, spectrum-dependent devices, main internet service provider inputs, mission-critical parts of the threat information network. The intelligence staff can determine key terrain in cyberspace by overlapping the threat's critical asset list, mission, and intent. <b>Note.</b> In cyberspace, it is possible for friendly and threat forces to occupy the same key terrain, potentially without either knowing of the other's presence.
Obstacles	Network features that can impede cyberspace operations include intrusion detection systems, firewalls, antivirus software, password protections, encryptions, reliability of network connectivity, data limits, and write-protections that prevent data manipulation.
Cover and concealment	The threat electromagnetic signature, cyberspace hygiene, noise awareness, and ability to limit attribution are considered cover and concealment within the cyberspace domain. Intelligence staffs determine collaboration or intelligence reach— If threat actors are hiding their true identity using multiple cyber-personas, honeypots, or Dark webs. Threat defensive measures (firewalls, software patches, antivirus software, encryption software, nonattributable proxy systems). Time and volume of network activity. These may support concealment of activity on the network.

*Ref: Table D-1. Terrain analysis and corresponding cyberspace considerations.*

### Civil Considerations

When analyzing the environment from a cyberspace perspective, apply civil considerations (ASCOPE) by cross-walking with the operational variables (PMESII-PT). When analyzing the cyberspace domain, intelligence staffs consider the informa-

# B. Cyber-Centric Activities & Outputs (Step 2)

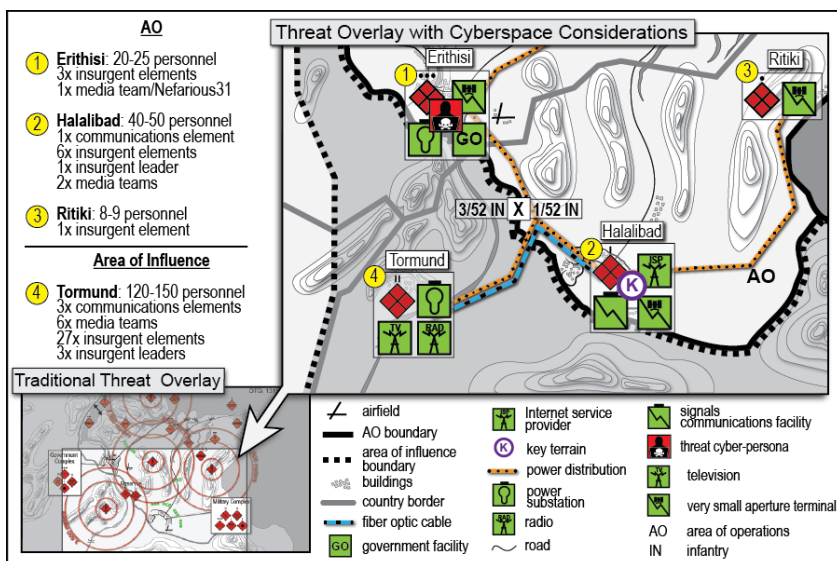
Ref: ATP 2-01.3, *Intelligence Preparation of the Battlefield* (Mar '19), pp. D-6 to D-9.

The S-2 ensures the intelligence staff accomplishes the following activities and outputs by the end of step 2, incorporating cyberspace considerations where applicable: threat overlay; threat description table; terrain analysis or MCOO; terrain effects matrix; weather, light, and illumination charts or tables; and civil considerations data files, overlays, and assessments.

## Threat Overlay

A threat overlay graphically depicts the threat's current physical location in the AO, AOI, and area of influence, including the threat's identity, size, location, and strength. A cyberspace perspective (see figure D-3) should evaluate—

- Physical and nonphysical AOs and AOIs by identifying the physical network layer, such as media communications infrastructure and server locations, and the logical network layer, such as hosts or the threat's use of social media sites or websites.
- Known or suspected physical or cyber-personas, threats, groups, or disseminating liaisons—size, strength, and physical or logical locations, if known or suspected.



Ref: ATP 2-01.3, fig. D-3. *Threat overlay with cyberspace components example.*

## Threat Description Table

A threat description table describes the broad capabilities of each threat depicted on the threat overlay (see table D-2). A cyberspace perspective should consider—

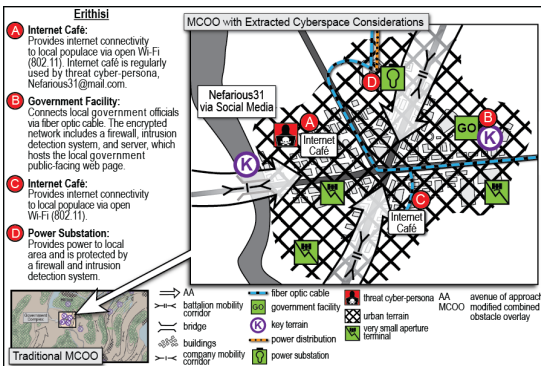
- Possible interdependencies between the threat's cyber and military capabilities (for example, the reliance on network communications infrastructure).
- Annotating any known or suspected technical capabilities, expertise, or programs.

Identity	Location	Disposition	Description
Nefarious31 (cyber-persona)	Erithisi	Operates from internet café as Nefarious31 using open Wi-Fi (802.11) weekly	<ul style="list-style-type: none"> <li>• Greatest cyber threat in the area of operations</li> <li>• Capable of offensive cyberspace operations using malware</li> <li>• Likely coordinating with government facility to increase cyber capability</li> <li>• Works closely with media elements to assist in propaganda/recruiting effort</li> </ul>
2x squads (16-18 personnel)	Erithisi government facility	Population provides sanctuary to threats	<ul style="list-style-type: none"> <li>• Armed conventional/irregular forces that protect government officials and secure government network</li> <li>• Government facility capable of distributed denial-of-service attack</li> </ul>
1x squads (8-9 personnel)	Erithisi southern boundary	Possible screening operations	Armed conventional/irregular forces that prevent U.S. forces from entering or occupying the area
Media element/ Recruitment	Erithisi	Operates from internet café using open Wi-Fi (802.11)	Disseminates threat propaganda to sympathetic population and actors in and around Erithisi, Ritiki, and Halalibad via social media and email campaigns

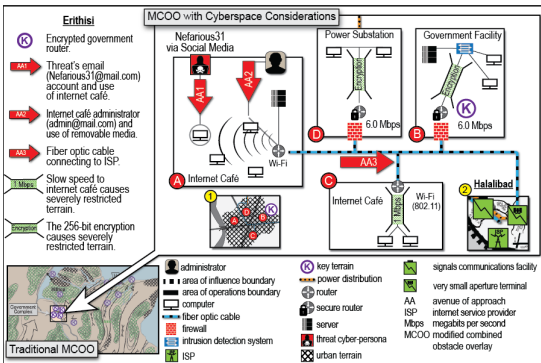
Ref: ATP 2-01.3, table D-2. Threat description table with cyberspace considerations example.

## Modified Combined Obstacle Overlay

The output from the terrain analysis is used to develop the MCOO, which should reflect the physical network, logical network, or cyber-persona layers of cyberspace when applicable. (See figures D-4 and D-5.) The MCOO traditionally includes natural and man-made OAKOC factors, built-up areas, and civil infrastructure. To add cyberspace considerations into a traditional MCOO, an intelligence staff should include (not all inclusive) public-switched telephone networks, radio stations, media kiosks, internet cafés, electric power, and other supervisory control and data acquisition systems.



Ref: Figure D-4. MCOO, physical network and cyber-persona layers example



Ref: Figure D-5. MCOO, physical network, logical network, and cyber-persona layers example.

# B. Cyber-Centric Activities & Outputs (Cont.)

Ref: ATP 2-01.3, *Intelligence Preparation of the Battlefield* (Mar '19), pp. D-6 to D-9.

*Note. Intelligence staffs, in conjunction with cyber support elements and echelons above corps, develop cyberspace considerations to the MCOO with organic assets. Fiber optic lines, which are physical connections that make it part of the physical network layer in cyberspace, are typically co-located or near existing LOCs, such as roads.*

## Terrain Effects Matrix

Using the MCOO as a guide, a terrain effects matrix describes OAKOC factor effects on friendly and threat operations. Table D-3 presents a terrain effects matrix for operations in the cyberspace domain.

OAKOC factors (military aspects of terrain)	Terrain effects with cyberspace aspects (As related to figures D-4 and D-5)
Observation and fields of fire	<ul style="list-style-type: none"><li>Internet café networks are wide-open and very accessible, thus allowing ability to see network configurations and the threat's capabilities.</li></ul>
Avenues of approach	<ul style="list-style-type: none"><li>Primary access through unencrypted, open Wi-Fi in internet cafés (Nefarious31 and administrator accounts).</li><li>Secondary access through regional internet service provider.</li></ul>
Key terrain	<ul style="list-style-type: none"><li>Regional internet service provider hosts regional power, radio, and television for area of operations.</li><li>Internet café router provides internet access to local populace, which is used to spread propaganda throughout the area of operations.</li></ul>
Obstacles	<ul style="list-style-type: none"><li>Intrusion detection systems, firewalls, secure routers, and 256-bit encryptions in both power substation and government facility.</li><li>Open Wi-Fi (802.11) in internet cafés with slow download and upload speeds (severely restricted).</li></ul>
Cover and concealment	<ul style="list-style-type: none"><li>Government network defended with intrusion detection systems, firewalls, secure routers, and encryptions.</li><li>Power substation also uses intrusion detection systems, firewalls, secure routers, and encryption.</li></ul>

Ref: ATP 2-01.3, table D-3. *Terrain effects matrix with cyberspace considerations example. A network component can be associated with more than one military aspect of terrain, such as a firewall that can be both an obstacle and provide cover from fires (on the network).*

## Weather, Light, and Illumination Charts or Tables

Weather, light, and illumination charts or tables describe weather, light, and illumination effects on friendly and threat operations. Potential cyberspace considerations comprise anyweather, including weather in space, that affects data transmissions, such as solar flares, high winds, and extreme weather conditions, such as sand storms, thunderstorms, or blizzards.

## Civil Considerations Data Files, Overlays, and Assessments

Civil considerations data files may include raw data such as voting locations, base locations, and organizational hierarchies. These data files support and are supplemented by civil consideration overlays, such as population and demographic overlays, and civil considerations assessments. Cyberspace considerations may include the use of non-governmental organizations to provide tacit or explicit support, such as proxy media disseminators or internet cafés. Additionally, consider the threat's use of government and noncombatant facilities for cyberspace or media activities or propaganda production.

Continued from previous page

Continued from previous page

tion and infrastructure variables. However, cyberspace operations affect, to varying degrees, the following civil considerations:

- **Areas:** In cyberspace, intelligence staffs should consider cellular phone coverage, internet service providers, and electricity distribution to industrial, commercial, and residential areas.
- **Structures:** Some cyberspace examples include power plants, moveable bridges and dams, communications/broadcast facilities (internet service providers, server farms, cell towers), internet cafés, and any building with an internet connection relevant to the AO or area of influence.
- **Capabilities:** For capabilities in cyberspace, consider internet access (and the capability to throttle or restrict access), cell phones, Wi-Fi, Bluetooth, fiber optic connections, cable television, modern information technological systems, internet and cellular network types.
- **Organizations:** Nonmilitary groups or institutions that can influence the AO (for example, hacktivists, community organizations, journalists, universities, and schools with a cyber curriculum, commercial and industrial unions, outside influencers or regional sympathizers, and online social media groups).
- **People:** Nonmilitary persons encountered by military personnel (for example, religiously and politically motivated hackers, network administrators, technologically proficient individuals, and commercial and industrial workers).
- **Events:** Routine, cyclical, historic, planned, or spontaneous activities and events that significantly affect organizations, people, and military operations.

## Step 3 — Evaluate the Threat

Intelligence staffs determine threat force capabilities, doctrinal principles, and TTP employed by threats in and through the cyberspace domain. The threats' use of cyberspace varies; they use the cyberspace domain differently to accomplish or support objectives. In step 3 of the IPB process, with input from individual intelligence disciplines, the intelligence staff evaluates the threat, creates threat models, develops broad threat COAs (attack, defend, reinforce, and retrograde) or capabilities in a narrative format, and identifies HVTs.

When creating a threat model that incorporates cyberspace considerations, identify how the threat has executed and integrated cyberspace operations independently of and in concert with traditional operations, and what the threat's capabilities are in and through cyberspace. It is also crucial to realize that the physical manifestation of the threat is not at the core of the threat. For example, where the threat appears is not necessarily where the threat is likely to be. Attributing an attack to a specific threat can be very difficult and consequently makes evaluating the threat especially challenging. For example, the use of a proxy allows the threat to conceal its true location. Tapping into intelligence reach assets is necessary to develop threat models that include TTP or signatures of different threats or groups in cyberspace.

### A. Step 3 Cyberspace Considerations

When evaluating the threat, understand that threats have varying cyberspace capabilities across all warfighting functions. However, the cyberspace domain likely affects each warfighting function to some degree. Therefore, it is prudent to evaluate how the threat uses the cyberspace domain to support operations by incorporating cyberspace considerations into each warfighting function to increase overall situational understanding. (See table D-4.)



Warfighting function	Cyberspace considerations
Command and Control	Delegation of authority, synchronization, and direction of forces throughout the cyberspace domain (for example, the use of email or websites to administer guidance to subordinate elements).
Movement and maneuver	Movement of forces, physically or logically, to achieve an advantage over a threat in the cyberspace domain (for example, the execution of a distributed denial of service to disrupt the threat's movement of forces).
Intelligence	The information derived through cyberspace, which enables understanding of the threat, terrain, or civil considerations (for example, the collection of threat open-source data).
Fires	The collective or coordinated use of indirect, cyberspace, missile defense, and joint fires through the targeting process (for example, the threat's use of offensive cyberspace operations or a threat's automated fire systems).
Sustainment	Cyberspace-enabled synchronized or coordinated support and services to enable freedom of maneuver, extending reach and endurance (for example, use of databases or cyberspace-enabled order processes of a threat's equipment or mission essential supplies).
Protection	Cyberspace-enabled methods to preserve the force, allowing commanders to apply maximum combat power (for example, the threat's use of defensive cyberspace operations to prevent geolocation or the targeting of its systems or networks).

Ref: ATP 2-01.3, table D-4. *Cyberspace considerations for the warfighting functions.*

In addition to considering and evaluating traditional threats on the battlefield, it is necessary to evaluate other relevant actors and threats that may conduct operations in cyberspace relevant to the AO:

- **Nation-state actors.** Nations that either conduct operations directly or outsource them to third parties to achieve national goals. They generally have access to domestic resources and personnel not typically available to other actors. They may involve traditional threats as well as traditional allies when conducting espionage.
- **Transnational nonstate actors or terrorists.** Formal and informal organizations not bound by national borders. These actors use cyberspace to raise funds, communicate, recruit, plan operations, destabilize confidence in governments, and conduct terrorist actions within cyberspace.
- **Criminal organizations or multinational cyber syndicate actors.** National or international, these criminal organizations steal information for their use or they sell it to raise capital. Nation states or transnational nonstate actors may use these criminal organizations as surrogates to conduct attacks or espionage through cyberspace.
- **Individual actors, hacktivists, or small groups.** These actors are known to illegally disrupt or gain access to networks or computer systems. Their intentions are as diverse as the number of groups or individual threats in cyberspace. These actors gain access to systems to discover vulnerabilities, sometimes sharing the information with owners. However, they may have a malicious intent. Political motivators often drive their operations, so they use cyberspace to spread their message. These actors can be encouraged or hired by others, such as criminal organizations or nation states, to conceal the attribution of those larger organizations.
- **Insider threats.** Any persons using their access wittingly or unwittingly to harm national security interests through unauthorized disclosure, data modification, espionage, or terrorism.

*Note. Friendly elements not practicing proper cybersecurity represent the greatest threat to friendly networks.*

## B. Cyber-Centric Activities and Outputs for Step 3

In step 3, the intelligence staff ensures the development of threat models—the primary outputs for this step that accurately depict how threat forces typically execute operations, and how they historically have reacted in similar circumstances relative to the specified mission and environment. The compilation of these threat models for each identified threat in the AO guides the development of threat COAs in step 4

of the IPB process. Step 3 may require the following IPB activities and outputs with cyberspace considerations, time permitting:

- Creating and updating threat characteristics files.
- Creating or refining the threat model.
- Creating a threat capability statement.

*Note. Upon completing steps 3 and 4 of the IPB process, update the intelligence estimate with current threat model details. Additionally, refine and update any requests for information or requests for collection.*

## Threat Characteristics

Analyze the threat in cyberspace applying the broad threat characteristics normally considered when analyzing any threat (see chapter 5 and appendix C). Cyberspace considerations may include—

- Attributing electronic devices to specific cyber-personas and/or persons.
- Social networking hierarchy.
- Historical threat TTP or malware signatures.
- C2 nodes.
- Threat intentions towards friendly networks.
- Insider threat potential from host-nation forces operating against friendly forces, or from a foreign intelligence physical threat.

## Threat Model

The threat model comprises three parts:

- Threat template.
- Threat tactics, options, and peculiarities.
- HVT identification.

*See following pages for further discussion of the threat model.*

## Threat Capabilities

Identify physical and nonphysical threats' operational patterns and capabilities in cyberspace by considering—

- If threats emit any unique electronic signatures.
- Media's production flow locally, regionally, and globally.
- If threats use any specific malware.
- Threats' or other relevant actors' skill level.
- Networks used to conduct operations and operations security.
- Threats' intent, for example, reconnaissance, espionage, and destructive malware.
- Threats' planning, scanning, and exploitation TTP.
- Threats' exfiltration TTP and their ability to move laterally across networks.
- Threat assets' C2.

Threat capability statements are used to identify threat capabilities, including cyberspace threat capabilities, and the broad options and supporting operations the threat can conduct to influence the accomplishment of friendly missions. This statement is a narrative that addresses an action the threat can complete. Major units may be portrayed on the threat template along with the activities of each warfighting function.

# Threat Model (& Cyber Kill Chain)

Ref: ATP 2-01.3, *Intelligence Preparation of the Battlefield* (Mar '19), pp. D-11 to D-13.

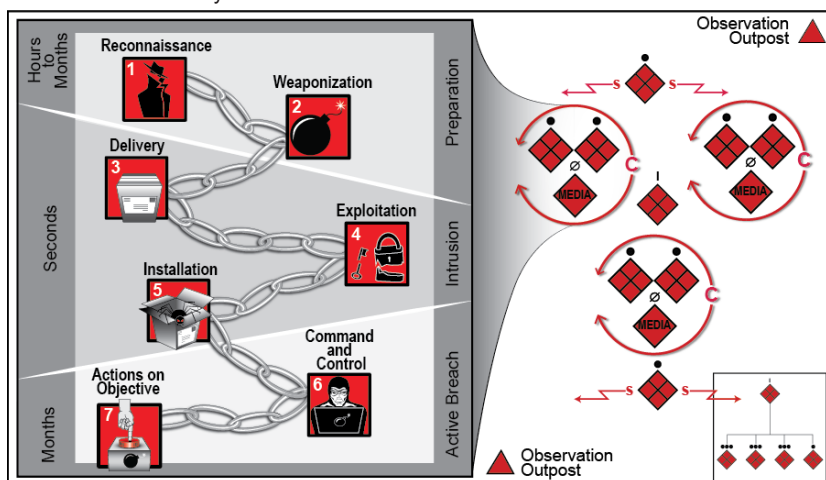
A threat template graphically depicts the threat's preferred deployment patterns, dispositions, and capabilities for a type of operation, when not constrained by OE effects. While there are several analytic programs, figure D-6 provides an example of a traditional threat template with cyberspace considerations using the Cyber Kill Chain methodology.

## Cyber Kill Chain

The Cyber Kill Chain is an analytic framework that describes the seven steps or the process the threat follows to achieve some offensive objective against a friendly network in cyberspace. Regarding IPB, it can be used as a cyber equivalency to a traditional threat template. It depicts a generalized, yet systematic approach that the threat takes to gain access to friendly resources in cyberspace when not constrained by OE effects. Understanding how attacks proliferate, the anatomy of cyberspace attacks, and historical pattern analysis of attackers in the AO can enhance the situational understanding of existing threats in cyberspace.

The following describes the seven phases of a Cyber Kill Chain:

- **Phase 1: Reconnaissance.** The threat collects information on the target before the actual attack begins.
- **Phase 2: Weaponization.** The threat exploits and creates or obtains a malicious payload to send to a victim associated with the targeted friendly network.
- **Phase 3: Delivery.** The threat sends the malicious payload to the victim by email or other means. This represents one of many intrusion methods the attacker can use.
- **Phase 4: Exploitation.** The threat exploits a vulnerability to execute code on the victim's system.
- **Phase 5: Installation.** The threat installs malware on the victim's system.
- **Phase 6: C2.** The threat creates a C2 channel to continue communications and operations of installed botnet or manipulation of the victim's system.
- **Phase 7: Actions on objectives.** The threat performs the steps to achieve goals inside the friendly forces' network.



Ref: ATP 2-01.3, fig. D-6. *Threat template with cyberspace considerations example.*

Although intelligence staffs have little to no capability to identify or detect activity related to the Cyber Kill Chain, this analytical framework provides a platform for them to articulate logically to commanders current and potential threats against friendly networks, as well as an attack's progress on the friendly network. The right half of figure D-6 depicts a generic threat formation for occupying a village or town without OE constraints. The left half of figure D-6 shows the steps and processes the threat's cyber element, which is imbedded with the threat's media element, takes to conduct a nondescript cyberspace attack against a friendly network.

*Note. The Cyber Kill Chain provides a common model for identifying and preventing cyber intrusions activity; however, the phases can occur nonsequentially.*

## Threat Tactics, Options, and Peculiarities

The threat model includes a description of the threat's preferred tactics. To assess threat tactics in cyberspace, identify—

- Similar TTP patterns against comparable networks worldwide.
- Any threats with the intent or capability to penetrate friendly networks, and the specific techniques they use.
- Threats' preferred methods of lateral movement.
- Any common malware used by any threat or threat elements.

## High-Value Targets

HVTs can be depicted and described on the threat template. HVTs related to cyberspace are identified and evaluated using the same resources as traditional methodologies—databases, intelligence studies, patrol debriefs, the threat template with supporting narrative, and tactical judgement. The intelligence staff's tactical judgement should be influenced and informed by performing a thorough CFA—normally associated with a center of gravity analysis—of the threat and other relevant actors. A CFA is one of the most useful structured analytic techniques to identify and frame the threat's capabilities in cyberspace. (See JP 5-0.) Additionally, in step 3, regarding general COAs identified in the threat model, a CFA assists in identifying HVTs in cyberspace.

**Critical Factors Analysis (CFA)** consists of three major areas, which are evaluated and analyzed:

- **Critical capability** is a means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s) (JP 5-0).
- **Critical requirement** is an essential condition, resource, and means for a critical capability to be fully operational (JP 5-0).
- **Critical vulnerability** is an aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects (JP 5-0).

*Note. A completed CFA may also act as the catalyst for another analytic tool—the (modified) CARVER criteria tool used in step 4 of the IPB process. (See chapter 5.)*

In evaluating HVTs, the intelligence staff should—

- Identify those assets critical to a threat's ability to conduct primary operations, sequels, or branches using cyberspace operations as a main effort or in a supporting role.
- When assessing HVTs in cyberspace, consider them based on the three layers of cyberspace (physical network, logical network, and cyber-persona).
- Identify those threat units explicitly tasked to conduct offensive cyberspace operations and those specifically tasked to conduct defensive cyberspace operations. The initial HVT list can be determined by mentally war-gaming and thinking through any specified operations under consideration.

## Step 4 — Determine Threat Courses of Action

In step 4, the final step of the IPB process, intelligence staffs identify and develop the full range of COAs available to the threat and describe threat COAs that can influence friendly operations. They develop the most likely and most dangerous COAs, incorporating cyberspace threats and considerations. The level of detail always depends on the time available.

It is essential to consider how threat COAs are fundamentally affected by the cyberspace domain. For example, upon identifying methods of threat communications, consider secondary and tertiary effects on threat COAs if any or all of those threat communications are denied through degraded, disrupted, destroyed, or manipulated. Identify HVTs for each COA, such as nodes, C2 centers, communications towers, satellites, internet service providers, fiber optic lines, and local power substations. Additionally, develop initial collection requirements for each COA.

### A. Step 4 Cyberspace Considerations

When determining threat COAs regarding cyberspace, consider—

- Threats' historical use of cyberspace and possible types of cyberspace operations conducted:
  - Malware—viruses, spyware, worms, network-traveling worms, socially engineered Trojans.
  - Password attacks—brute-force and dictionary attacks.
  - Denial-of-service or distributed denial-of-service attacks.
  - Advanced persistent threat.
  - Phishing attacks.
- Specific units with a task and purpose to produce cyberspace effects in the cyberspace domain.
- Threats' ability and desire to employ cyberspace operations against specific friendly operations.
- If threat forces will be arrayed distinctively based on cyberspace operations or effects.
- Threats that may be located outside of the AO.
- Threat COAs that may use proxies worldwide, which may be outside of the AOI.
- COAs that address the use of the cyberspace domain in completely different ways.

### B. Cyber-Centric Activities and Outputs for Step 4

At the end of step 4, the S-2 ensures the intelligence staff accomplished the following IPB activities and outputs, including cyberspace considerations, as time allows:

- Refined threat COA statement.
- Threat situation template.
- Event template and event matrix:
  - Identify potential objectives, decision points, NAIs, and TAIs.
  - Provide input to the information collection plan.
  - HVT list and input to the HPT list.

## Refined Threat Course of Action Statement

The refined threat COA statement is a narrative that describes the situation template. It should typically contain—

- The threat situation, mission, objectives and end state, and task organization.
- Capabilities.
- Vulnerabilities.
- Decision points.
- The decisive point.
- Failure options.

Each of these categories should be considered from a cyberspace perspective, either integrating a cyberspace narrative into each category or creating a separate cyberspace narrative at the end of the threat COA statement. Use the technique that best describes the threat's use of cyberspace to the commander. The level of emphasis on cyberspace should be comparable to the threat's use of and effectiveness in cyberspace.

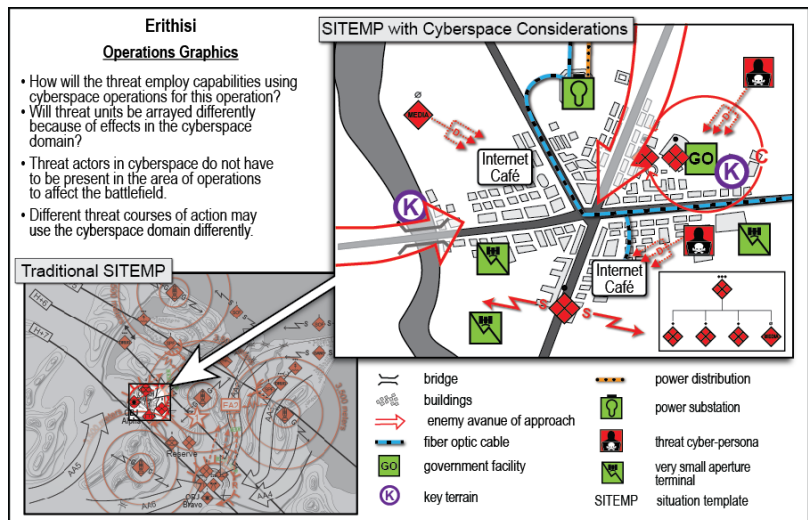
## Threat Situation Template

The threat situation template is a graphic overlay that depicts the threat's expected disposition upon the threat's selection of a COA. Typically, the situation template is accomplished by overlapping the threat template with the MCOO, which incorporates environmental effects on operations, and displaying the threat executing a specific COA.

In cyberspace, the situation template can depict a threat that is physically located within the AO and integrated with regular threats, as shown in figure D-7 below. It can also be depicted from the physical network layer perspective, which may also contain logical network elements, as shown in figure D-8 on p. 4-r.

The level of cyberspace detail in the situation template should be proportional to the level of the threat in cyberspace and the friendly unit's mission.

*Note. Threats associated with cyberspace may be integrated with larger, regular threats, or they may be independent entities with no known connection to the local threat.*



Ref: ATP 2-01.3, fig. D-7. Threat situation template with cyberspace considerations, example 1. See p. 4-r for a second example (fig. D-8).

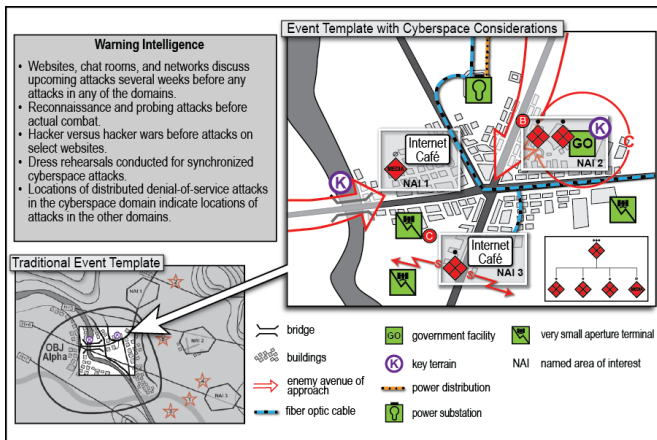
# Event Template and Event Matrix

Ref: ATP 2-01.3, *Intelligence Preparation of the Battlefield* (Mar '19), pp. D-16 to D-18.

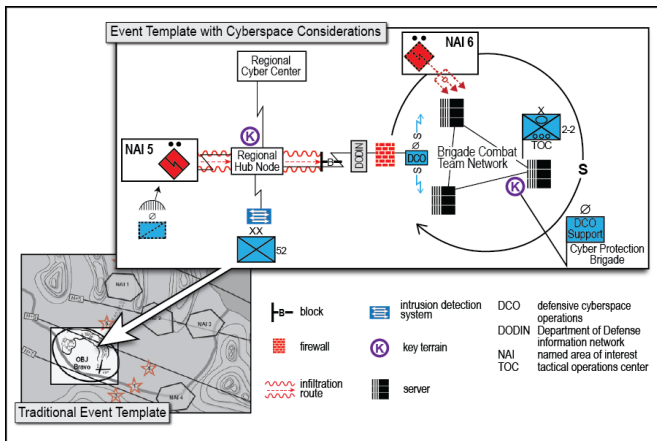
An event template is a graphic overlay that confirms or denies threat COAs. This enables the development of the information collection plan. An event matrix always accompanies the event. The event template traditionally results from overlapping the developed situation templates to identify those areas or indicators that identify a COA as being unique. Prominent differences are marked as NAIs. In contrast, NAIs in cyberspace are likely not determined by overlapping situation templates and can be physical or logical.

In cyberspace, as in the land, air, maritime, and space domains, a historical record of TTP on how the threat fights assists in determining NAIs, showing possible, expected activity at a specified location. Consider that NAIs regarding cyberspace are likely related to locations or activity on a network—possibly indicating a specific type of cyberspace operations. Each NAI is linked to an assigned task and the party responsible for collecting and reporting any illicit activity or items associated with those NAIs.

*Note. It is not possible to stop all malicious activity on a network. A determination should be made between which systems are mission-critical and need to be secured, versus systems that just need to be monitored.*



Ref: ATP 2-01.3, fig. D-9. Event template with cyberspace considerations, example 1. Figure D-9 illustrates an event template with developed NAIs for a local threat present in the AO.



Ref: ATP 2-01.3, fig. D-10. Event template with cyberspace considerations, example 2. Figure D-10 illustrates the same threats attacking a friendly network, primarily focused on the physical network layer aspect.



## Event Matrix

An event matrix describes indicators and activity expected to occur in each NAI. Although there is no prescribed format for the event matrix, it normally associates each NAI and threat decision point with indicators and the times they are expected to occur, as well as COAs they confirm or deny. (See table D-5.)

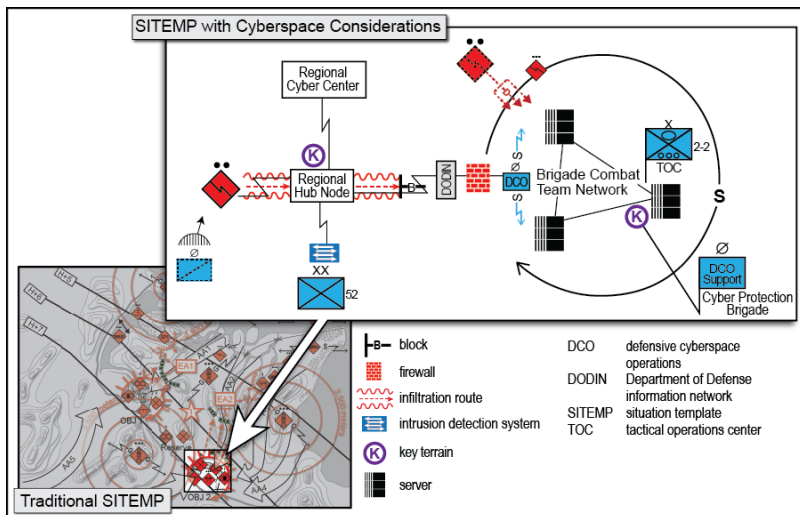
The time that a threat activity may or may not occur in cyberspace is likely influenced more by intangible variables such as the stealth and persistence of the resource being used (for example, the malware designated for an attack):

- Stealth of the resource refers to the probability that if the threat uses the resource, the resource will still be available for use in the future.
- Persistence of the resource refers to the probability that if the threat refrains from using the resource, the resource will still be useable in the future.

The timing of a threat's cyberspace attack is tied less to typical environmental factors (such as increased visibility due to daylight)—which are considered imperative for some traditional operations—and more to the logical aspects of the network. For example, the volume of network activity may spur threat operations because it can mitigate attribution, which increases stealth.

<i>Named area of interest</i>	<i>Indicators</i>	<i>Threat decision point</i>	<i>Time</i>	<i>Threat course of action indicated</i>
1	<ul style="list-style-type: none"> <li>• Uses email</li> <li>• Targeting is specific</li> <li>• Sophisticated, appears to come from associate, client, or acquaintance</li> <li>• May be contextually relevant to work</li> </ul>	1	Time of cyberspace operations may be synchronized with land or other operations.	Spear-phishing attack
2	<ul style="list-style-type: none"> <li>• Unusually slow network performance</li> <li>• Unavailability of a particular website</li> <li>• Unable to access any website</li> <li>• Stark increase in the number of spam emails received (also known as an email bomb)</li> </ul>	2	Cyberspace operations may be planned over a period of months or years	Denial-of-service attack
3	<ul style="list-style-type: none"> <li>• Social media sites contain an increase in negative messaging</li> <li>• Intelligence assets discover different media in the area of operations containing threat messaging</li> </ul>	3	<ul style="list-style-type: none"> <li>• Timing may be seasonal or synchronized with other threat operations</li> <li>• Timing may be linked to negative effects of friendly operations</li> </ul>	Propaganda campaign

Ref: ATP 2-01.3, table D-5. Event matrix with cyberspace considerations example.



Ref: ATP 2-01.3, fig. D-8. Threat situation template with cyberspace considerations, example 2.

# I(b). Requesting Cyberspace Effects (CERF)

*Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), app. E.*

In conjunction with the necessary legal and operational authorities, commanders select organic EW capabilities to create desired effects on targets identified for EAs. If a unit's organic EW capabilities do not fulfill the targeting requirements to support the commander's intent, or if the commander does not have the authority to employ a particular EW capability, the CEMA section requests support from the next higher echelon. To request EA that will be administered by aircraft, the CEMA section uses the Joint Tactical Air Strike Request and the support request tool.

As requests pass from echelon to echelon, each echelon processes the Joint Tactical Air Strike Request to assess their ability to provide the support that meets the requesting unit's requirements. The requirement elevates either until it reaches an echelon that can support the requesting unit or until the highest echelon denies the request. Supporting a requesting unit may not be possible due to prioritization, timing, capabilities, authorization, or conflict with other EW capability requirements. Commanders ultimately have the responsibility for denying resource requests and may delegate that authority to their staff. The joint force commander may refuse a request for joint air resources, but not the joint force air component commander.

*See pp. 4-27 to 4-28 for discussion of electromagnetic attack requests to include DD Form 1972 (Joint Tactical Air Strike Request).*

Corps and below units do not have organic cyberspace capabilities to conduct DCO-IDM, DCO-RA, or OCO missions. The G-3 or S-3 requests support through higher headquarters. The G-6 or S-6 and the CEMA section coordinate to request DCO-IDM after determining that a threat in friendly cyberspace is beyond the scope of cyberspace security. DCO-IDM is an enabler for DCO-RA. Cyber mission forces performing DCO-IDM request DCO-RA upon deciding that a cyberspace threat requires a defensive attack beyond friendly cyberspace. OCO is used to create desired effects on targets identified for cyberspace attacks on the integrated target list. DCO-RA and OCO are similar except that DCO-RA is only used to deter a threat, whereas OCO is used to project power.

## I. Requesting Cyberspace Effects (CERF)

Cyber Effects Request Format (CERF) is the format corps and below units use to request cyberspace support. Support in response to a CERF may come from joint cyberspace forces such as the combat mission teams, from other joint or Service capabilities, or Service-retained cyberspace forces.

### Effects Approval at Echelons Corps and Below

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 specific targets. If the requesting and higher echelons determine that a current capability is insufficient, the commander and staff approve and processes the CERF. The routing process continues to each echelon until the CERF reaches the joint force land component command it is converted to an RFS, and forwarded to the JTF headquarters. The CERF approval process at echelons corps and below follow the below steps—

- Identify targets of cyberspace effects.
- Verify if organic capabilities can create desired effects.

- Approve target for cyberspace effects.
- Forward to next higher Army echelon for deconfliction and synchronization.
- Verify if other organic capabilities can create desired effects if organic cyberspace capabilities do not exist.
- If current capabilities fulfill the requirement, synchronize operations.
- If current capabilities do not fulfill the requirement, approve target for cyberspace effects.
- Forward to next higher Army echelon for approval until CERF enters the joint process.
- Synchronize operation with cyberspace effect (if possible).

*Note. The joint force land component command may require the requesting corps to convert the CERF to an RFS format before submitting it into the joint process.*

## Effects Approval at Echelons Above Corps

Cyberspace operations provide a means by which Army forces can achieve periods or instances of cyberspace superiority to create effects to support the commander's objectives. Cyberspace attack capabilities are tailored to create specific effects and must be planned, prepared, and executed using existing processes and procedures. Commander and staff at all echelons apply additional measures for determining where, when, and how to use cyberspace effects.

Commanders and staff at each echelon will coordinate and collaborate regardless of whether the cyberspace operation is directed from higher headquarters or requested from subordinate units. The Army intelligence process, informed by the joint intelligence process, provides the necessary analysis and products from which targets are vetted and validated, and aim points are derived. As a result of the IPB process, and in collaboration with the joint intelligence preparation of the operational environment process, intelligence personnel develop network topologies for enemy, adversary, and host nation technical networks.

Targets determined during the planning process are described broadly as physical and logical entities in cyberspace consisting of one or more networked devices used by enemy and adversary actors. The G-2 may label these targets as named areas of interest and target areas of interest. Additionally, an analysis of friendly force networks will inform the development of critical information and provide a basis for establishing key terrain in cyberspace. Critical network nodes are key terrain in cyberspace. They include those physical and logical entities in friendly force technical networks of such extraordinary importance that any disruption in their operation would have debilitating effects on accomplishing the mission.

As part of CEMA, the staff will perform a key role in target network node analysis. While determining cyberspace attack effect-types for targets and defensive measures for critical network nodes, the CEMA section will prepare, submit, and track the CERF. This request will elevate above the corps echelon and integrate into the joint targeting cycle for follow-on processing and approval.

# Cyber Effects Request Format (CERF)

Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), fig. C-2.

Format 26. Cyber Effects Request Format (CERF)				
SECTION 1 REQUESTING UNIT INFORMATION				
SUPPORTED MAJOR COMMAND:		DATE:	TIME SENT:	
REQUESTED UNIT:		BY:		
POINT OF CONTACT::		CLASSIFICATION (Unclassified Until Filled in)		
USCYBERCOM J3 USE ONLY:				
SUPPORTED OPLAN/COMPLAN/ORDER:		RECEIVED BY JOC		
SUPPORTED MISSION STATEMENT:		DATE:	TIME:	
SUPPORTED COMMANDER'S INTENT:		NAME/RANK:		
SUPPORTED COMMANDER'S ENDSTATE		CERF TRACKING NUMBER:		
SUPPORTED CONCEPT OF OPERATION:		ASSIGNED TO:		
SUPPORTED OBJECTIVE (STRAP/OP/TACT):		STAFF SECTION:		
SUPPORTED TACTICAL OBJECTIVE/TASK		DATE:		
		TIME:		
		POC:		
		REMARKS:		
SECTION 3 - COMPUTER NETWORK OPERATIONS (CNO) SPECIFIC INFORMATON				
TYPE OF TARGET:		TARGET PRIORITY:		
SCHEDULED	ON-CALL	EMERGENCY	PRIORITY	ROUTINE
TARGET NAME:		TARGET LOCATOR		
TARGET DESCRIPTION:		DESIRED EFFECT:		
TARGET FUNCTION:		TARGET SIGNIFICANCE:		
TARGET DETAILS: Include any relevant device information such as type; operating system version and patch level, software, number of users, activity, friendly actors in the area of operations, surrounding/adjacent/parallel devices, etc.				
CONCEPT OF CYBER OPERATION: Include Task, Purpose, Method and Endstate. Also specify intelligence collection plan for battle damage assessment (BOA), to include allocated resources, measures of performance (MOPs), measure of effectiveness (MREs), and Measures of Effectiveness indicators (MOEs).				
TARGET EXPECTATION STATEMENT:				
REMARKS: If any of the following information is available, please provide 1.) Time on target/Duration of Effect 2.) No Earlier Than/No Later Than Need Time 3.) Trigger Event, or Conditions for Execution 4.) Persistence Requirement (ie., effect must persist through a restart of the target, trigger event) ) 5.) Command and Control Requirement (ie., effect must be able to be turned on/off remotely) 6.) Self-Destruct / Auto Delete Requirement (ie., effect must stop itself if C2 is lost after X amount of time) 7.) Level of Attribution Requirement (ie., unattributable to CONUS or USG, misattributed, attributed to USG, etc) 8.) Level Desectability allowed (ie., should not be detected by (a) administrator, (b) user © forensic analyst, etc) 9.) Level Co-optability allowed (ie., low, medium, high) 10.) Remote Monitoring Requirement (ie., effect should be able to be monitored by (a) operator, (b) JOC, etc) 11.) Infrastructure Requirement (ie., effect should be launched from (a) National Security Agency (NSA) Tailored Access Operations (TAO) (b) naval vessel, etc) 12.) Reversability Requirement (ie., effect should be reversible/not reversibility)				

Planning  
(Cyber & EW)

## II. Cyber Effects Request Format Preparation

Although the requesting unit may not have the specific target network topology information it should provide current target information. The approval process for cyberspace effects may take longer than other targeting capabilities.

*Figure C-2 (previous page) shows an example the format and instructions required to complete the CERF. The requesting unit will complete all sections except the USCYBERCOM operations directorate of a joint staff (J-3) portion of the CERF as described below.*

### A. Cyber Effects Request Format Section 1 Requesting Unit Information

Section 1 of the CERF requests the following unit information—

- Supported Major Command. Enter the major command authorized to validate and prioritize the CERF. For Army units at corps level and below this entry will commonly include the geographic or functional combatant command.
- Date. Enter the date the completed CERF(s) are submitted to higher headquarters.
- Time Sent. Enter the time the CERF is submitted to higher headquarters.
- Requesting Unit. Enter the name of the unit originating the requirement for the creation of effect(s) or conduct of specific activities.
- By. Enter the rank, last, and first name of the unit point of contact that time stamped and processed the CERF.
- Point of Contact. Enter the rank, last, and first name of the unit point of contact from the requesting unit. Also, enter phone number and e-mail.
- Classification. Enter the overall classification of the document. Ensure classification markings are applied to each section and supporting documentation.

### B. Cyber Effects Request Format Section 2 Supported Operation Information

Section 2 of the CERF requests the following supported operation information—

- Supported OPLAN/CONPLAN/Order. Describe key information within the plan that the requested effect(s) will support.
- Supported Mission Statement. Describe the unit's essential task(s) and purpose that the requested effect(s) will support.
- Supported Commander's Intent. Describe key information within the commander's intent that the requested effect(s) will support.
- Supported Commander's End State. Describe key information within the commander's end state that the requested effect(s) will support.
- Supported Concept of Operations. Describe key information within the concept of operations that the requested effect(s) will support.
- Supported Objective (strategic, operational, and tactical). Describe the supported objective(s) that the requested effect(s) will directly support.
- Supported Tactical Objective/Task. Describe the tactical objectives and tasks that the requested effect(s) will directly or indirectly support.

## **C. Cyber Effects Request Format Section 3**

### **Computer Network Operations**

Section 3 of the CERF requests the following computer network operations and specific information—

#### **Type of Target**

- Indicate “scheduled” if specific dates, times, and or supporting conditions are known.
- Indicate “on-call” if trigger events or supporting conditions are known.

#### **Target Priority**

- Indicate “emergency” if target requires immediate action. Indicate “priority” if target requires a degree of urgency.
- Indicate “routine” if target does not require immediate action or a degree of urgency beyond standard processing.

#### **Target Name**

Enter name of target as codified in the Modernized Integrated Database.

#### **Target Location**

- Provide target location according to CJCSI 3370.01, Enclosure D.
- Disregard if the request is for specific activities to support DODIN operations or DCO.

#### **Target Description**

- Provide target(s) description according to CJCSI 3370.01, Enclosure D.
- Provide description of network node(s) wherein specific activities are to support DODIN operations or DCO.

#### **Desired Effect**

- Enter deny, degrade, disrupt, destroy, or manipulate for OCO.
- Provide timing as “less than 96 hours”, “96 hours to 90 days”, or “greater than 90 days”.

#### **Target Function**

Enter target(s) primary function and additional functions if known.

#### **Target Significance**

Describe why the target(s) is important to the enemy’s or adversary’s target system(s) and/or value in addition to its functions and expectations.

#### **Target Details**

Describe additional information about the target(s) if known. This information should include any relevant device information such as type; number of users; activity; friendly actors in the area of operations; and surrounding/adjacent/parallel devices.

#### **Concept of Cyberspace Operations**

Describe how the requested effect(s) would contribute to the commander’s objectives and overall concept of operations.



- Include task, purpose, method, and end state.
- Describe the intelligence collection plan and specific assessment plan if known.
- Provide reference to key directives and orders.

## Target Expectation Statement

According to CJCSI 3370.01, Enclosure D, describe how the requested effect(s) will impact the target system(s). This description must address the following questions.

- How will the target system be affected if the target's function is neutralized, delayed, disrupted, or degraded? (Two examples are operational impact and psychological impact.)
- What is the estimated degree of impact on the target system(s)?
- What is the functional recuperation time estimated for the target system(s) if the target's function is neutralized, delayed, disrupted, or degraded?
- What distinct short-term and/or long-term military or political advantage/disadvantage do we expect if the target's function is neutralized, delayed, disrupted, or degraded?
- What is the expected enemy or adversary reaction to affecting the target's function?

# II(a). Electronic Warfare Planning

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), chap. 3.

## I. Electronic Warfare Contributions to the Military Decision-Making Process

EW planners follow the MDMP. In a time-constrained environment, they follow the abbreviated MDMP appropriately. The CEWO ensures planned EW activities contribute to the operation. Staff planners with the necessary expertise, and in some cases access to sensitive compartmented information facilities, are essential for planning EW and related capabilities. Integrating EW into operations requires placing planners at the brigade combat team level with experience in capabilities, such as special technical operations and special access program effects. Throughout the MDMP, the CEWO continuously identifies risks and appropriate risk mitigation techniques.

The CEWO participates in the MDMP by planning and synchronizing EW and cyberspace operations actions. During planning, the CEWO considers joint, interorganizational, and multinational dependencies and interdependencies of EW resources.

The members of the CEMA section assist the CEWO during the MDMP by conducting terrain and radio wave propagation analysis relevant to friendly and threat forces within an operational environment. The results of the analysis contribute to staff products, such as map overlays depicting EW assets and their associated range of effectiveness. The staff uses the products to refine the EW portions of the plan. The CEMA section builds and staffs operations order appendices and annexes and submits them to the G-3 (S-3) staff for dissemination. The CEWO provides EA information to the fires staff for inclusion in Annex D of the operations order (FM 6-0).

The CEMA section considers policies, laws, and ROE that affect EW operations when participating in the MDMP process. The SJA and the CEMA working group develop the ROE for commander review. Planners and the SJA clarify the ROE or develop supplemental ROE when necessary.

*See pp. 4-2 to 4-8 for discussion of EW operations (and cyberspace operations) planning and the MDMP.*

## II. Electronic Warfare Planning Considerations

Several considerations are important to planning EW operations to include equipment type, configurations, logistics, availability, and risks. The running estimate is a tool to assist with planning and maintaining awareness of EW capabilities, current missions, and future mission requirements.

*See following pages (pp. 4-16 to 4-17) for discussion of the EW running estimate.*

### A. Planning Factors

The CEWO visualizes an operational environment and EME using maps and simulation programs that predict the behavior of radio waves used during unified land operations. The course of action proposed by the CEWO requires analysis to determine the capabilities and limitations of the systems. For example, man-pack EW systems are lightweight and highly mobile but also have limited transmit power for EA. Vehicle mounted systems allow for higher power output but have line of sight (LOS) limitation in dense terrain.

## B. Electronic Warfare Running Estimate

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 3-3 to 3-5.

The CEWO prepares and continually updates the running estimate. 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). Information in the running estimate are committed and reserved assets, maintenance status of EW equipment and training proficiency of EW personnel. Resources that are useful in developing a running estimate are the maintenance report and the commanders' training assessments. Threat information is available from online databases, unit intelligence assets, and national intelligence sources.

The purpose of the CEMA section running estimate is to provide a consolidated list of information about cyberspace and the electromagnetic spectrum to assist the CEMA section in planning, preparing, and executing operations. The information serves as a foundation for the Appendix 12 to Annex C and tabs, and is dependent on information requirements with other staff such as Operations, Fires, Intelligence, and Signal as sources of information. Some of this information will be redundant with other staff section planning products. Table 3-1 below is an example of an EW running estimate.

1. Friendly electronic warfare systems.
  - a. System nomenclature and disposition by echelon.
    - i. Planning, modeling, and simulation tools.
    - ii. Organic systems.
    - iii. Echelons above corps and joint assets.
  - b. System capabilities.
    - i. Frequency range.
    - ii. Modulation type(s).
    - iii. Maximum power output.
    - iv. Antenna configuration and characteristics.
    - v. Command and control details (mesh network parameters, data paths, and bandwidth requirements).
  - c. Modeling and simulation of each system based on differing parameters and area of operations
    - i. Differing power ratios.
    - ii. Antenna configuration.
    - iii. Terrain.
  - d. Constraints and limitations associated with each system.
2. Friendly spectrum-dependent systems.
  - a. System nomenclature and disposition by echelon.
    - i. VHF radios
    - ii. Satellite communications terminals.
    - iii. Radar sets.
    - iv. Unmanned aircraft systems
  - b. System characteristics.
    - i. Frequency ranges.
    - ii. Bandwidth requirements.

- iii. Power.
  - iv. Modulation.
- c. Modeling and simulation of each system, based on differing parameters and area of operations.
- d. Constraints and limitations associated with each system.
- 3. Friendly electronic warfare systems.
  - a. System nomenclature and disposition by echelon.
  - b. System capabilities.
    - i. Frequency range.
    - ii. Modulation type(s).
    - iii. Maximum power output.
    - iv. Antenna configuration and characteristics.
    - v. Command and control details (mesh network parameters, data paths, and bandwidth requirements).
  - c. Threat electronic warfare tactics, techniques, and procedures.
  - d. Modeling and simulation of each system, based on differing parameters and area of operations.
  - e. Critical capabilities and vulnerabilities by system.
- 4. Threat spectrum-dependent systems.
  - a. System nomenclature and disposition by echelon.
  - b. System characteristics.
    - i. Frequency ranges.
    - ii. Bandwidth requirements.
    - iii. Power.
    - iv. Modulation.
  - c. Tactics, techniques, and procedures.
  - d. Frequency allocations.
  - e. Cueing cycles (radar sets)
  - f. Modeling and simulation of each system, based on differing parameters and area of operations.
  - g. Critical capabilities and vulnerabilities by system.
- 5. Civil infrastructure considerations.
  - a. Networks in the area of operations.
    - i. SCADA.
    - ii. Internet service providers.
    - iii. Fiber (regional, national, and international).
  - b. Spectrum resources and allocations (with characteristics of each).
    - i. Wi-Fi.
    - ii. Broadcast television.
    - iii. Broadcast radio.
    - iv. Satellite ground stations.
  - c. Physical access to structures and equipment.

*Ref: ATP 3-12.3, Electronic Warfare Techniques (Jul '19), table 3-1. Example of an electronic warfare running estimate.*

Airborne platforms offer the best LOS of EW systems, but are vulnerable to enemy air defense systems and have limited dwell time on target.

## Additional Factors for Airborne Planning

Maintenance activities and other missions reduce the availability of aircraft to support EW requirements. Airborne platform unavailability for EW is attributed to—

- Poor weather and visibility that restrict flight.
- Planned and unplanned maintenance.
- Transport missions.
- Intelligence, surveillance, and reconnaissance missions.
- Communications missions.

## Logistical Considerations

Units conduct scheduled and unscheduled maintenance on EW equipment. Maintenance ensures readiness for current and future operations. The CEWO, with assistance from logistics staff, develops an SOP that includes maintenance procedures. The CEWO or representative prioritizes maintenance efforts ensuring a unity of effort, as maintainers are a limited resource.

The planner considers—

- An EW capability replacement plan for potential coverage gaps and unexpected outages.
- Parts availability for maintenance to prevent non-mission capable equipment.
- Power resources including:
  - Batteries.
  - Generators and fuel.
  - Shore power.
  - Vehicle or transport power sources

Commanders allocate EW resources to support various units. When EW resources support another unit, the supported unit—

- Identifies EW requirements.
- Protects and defends EW assets.
- Provides logistical support.

## Risk Management

EW can cause unwanted radio frequency (RF) exposure to personnel. High levels of RF exposure can damage external and internal human tissue. The CEWO identifies risks associated with EW activities and develops mitigating steps to reduce the risk to friendly personnel and equipment. The CEWO then coordinates with the staff to refine the risk mitigating recommendations and presents them to the commander. For more information about risk management, refer to ATP 5-19.

Planners synchronize EW with lethal and nonlethal capabilities to achieve desired effects. The CEWO uses predetermined formulas to calculate EA and ES.

*For additional information on predetermined formulas and jamming calculations, refer to ATP 3-12.3, Electronic Warfare Techniques (Jul '19), appendix B.*

EW actions can mitigate operational risk, though using EA, both offensively and defensively, has inherent risk associated with the systems due to emissions. The risks include hazards of electromagnetic radiation to personnel, hazards of electromagnetic radiation to fuels, and hazards of electromagnetic radiation to ordnance.

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 RF energy above certain power levels in certain frequency bands for certain lengths of time. DODI 6055.11 specifies the allowable amounts of radiation and personnel exposure time to RF fields at particular intensities and frequencies.

Hazards of electromagnetic radiation to fuels is the hazard associated with the possibility of igniting fuel or other volatile materials through RF energy-induced arcs or sparks. It takes a certain amount of arc energy to ignite a fuel, and modern fuels are much safer than older fuels. This is a major concern when there is limited separation between EW capabilities and fuel, such as airfields, forward armament and refueling point, and refueling on-the-move locations. Fortunately, there are many operational safeguards against this problem.

Hazards of electromagnetic radiation to ordnance refers to the susceptibility of electro-explosive devices to RF energy. Electro-explosive or electrically-initiated devices are the control devices to detonate explosives, launch ejection seats, cut tow cables, and other similar functions. Modern communications and radar transmitters can produce high levels of electromagnetic energy that are potentially hazardous to ordnance. These environments can cause premature actuation of sensitive electro-explosive and electrically initiated devices.

### III. Staff Contributions to EW Planning

EW personnel are dependent on the staff for a variety of products to understand an operational environment, targeting, and EP requirements. The EW personnel can plan EW activities once they have sufficient situational awareness of an operational environment.

*See following pages (pp. 4-20 to 4-21) for an overview and discussion of EW Contributions to the staff.*

#### A. G-2 (S-2) Staff

EW planners rely on the G-2 (S-2) staff for threat characteristics identified during IPB. The CEWO submits requests for information to address gaps identified during IPB.

In most cases, the CEWO relies on SIGINT-derived enemy electronic technical data to plan and conduct EW targeting operations. Therefore, the G-2 (S-2) staff supports the CEWO during the alignment of EW and SIGINT assets against the commander's priorities of effort to achieve the best possible outcomes. SIGINT and EW resources, synchronized with the commander's scheme of maneuver significantly, enhances situational awareness while increasing the precision of the targeting process. For more information about a line of bearing (LOB), a cut, and a fix, see paragraph 5-8.

Useful products G-2 (S-2) creates or assists in creating include—

- High-value target list (HVTL) during IPB.
- High-payoff target list (HPTL) during MDMP.
- Enemy electronic order of battle (EOB).

#### B. G-6 (S-6) Staff

The CEWO uses the joint restricted frequency list (JRFL) and friendly network architecture to plan EW and avoid EMI. The CEWO and the G-6 (S-6) use this information to develop the unit EP plan.

*See p. 4-22 for an overview and discussion of the joint restricted frequency list (JRFL).*

# EW Contributions to the Staff

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 3-9 to 3-11.

The CEWO provides information to other staff sections to aid in planning. This information answers requests for information and aids in refining staff products.

## Contributions to G-2 (S-2) Staff

The CEWO contributes to the IPB and throughout the MDMP by providing input related to EW activities. IPB involves systematically and continuously analyzing the threat and certain mission variables (terrain, weather, and civil considerations) in the geographical area of a specific mission. Commanders and staffs use IPB to gain information that supports understanding. Some of the CEWO's input to the IPB includes the following:

- Information regarding how the EME affects operational environments.
- Input to likely threat COAs by providing information on threat EMS capabilities, tactics, techniques, and procedures.

When evaluating how the EME affects an operational environment, the CEWO—

- Analyzes the EME and identifies known or suspected threat emitters of interest and neutral emitters in the area of operations.
- Identifies facilities, which may support, operate, or house enemy EW capabilities.
- Contributes to the G-2 (S-2) understanding of the enemy's use of the EMS.

When describing the effects of an operational environment on EW activities, the CEWO—

- Conducts terrain analysis of both the land and air domains using the factors of observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, and cover and concealment.
- Identifies terrain that protects communications and target acquisition systems from activities. Terrain masking reduces friendly vulnerabilities to threat EW actions.
- Identifies how terrain affects LOS, including effects on both communications and noncommunications transmitters. Line of sight is the unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another (ATP 2-01.3).
- Evaluates how vegetation affects radio wave absorption and antenna height requirements.
- Locates power lines and their potential to interfere with radio waves.
- Assesses the likely air and ground avenues of approach, their dangers, and potential support that EW activities could provide for them.
- Determines how weather (including visibility, cloud cover, rain, and wind) may affect ground-based and airborne EW activities and capabilities (for example, when poor weather conditions prevent airborne EW launch and recovery).
- Assists the G-2 (S-2) staff with the development of the modified combined obstacle overlay.
- Considers all other relevant aspects of an operational environment that affect EW activities, using the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time) and mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations).

The CEWO contributes to the G-2 (S-2) staff's understanding during enemy course of action development by providing—



- Subject-matter-expert input on enemy EW tactics, techniques, and procedures for situation template development.
- A review of named areas of interest and target areas of interest to confirm EW considerations.
- EW options to support decision points.
- EW input to the event template and event matrix.

## Contributions to Other Staff

During planning, the CEWO provides information to other members of the staff including—

- EW input to IPB [G-2 (S-2)] staff.
- Input to the HPTL (Fires).
- Input to the commander's critical information requirements including essential elements offriendly information and priority intelligence requirements [G-2 (S-2) and G-3 (S-3)] staff.

## Contribution to Fires (Targeting Working Group)

The targeting working group recommends priorities for the targets according to its judgment and the advice of the fires cell, targeting officer and the field artillery intelligence officer. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting working groups maintain a HPTL and inform the commander of targets that do not support the commander's guidance. The HPTL includes the recommended priority of targets and target engagement sequence. The HPTL includes the target category, a name, or a number.

The CEWO recommends to the G-3 (S-3) staff and the fire support element whether to engage a target with EW. The fires support element uses decide, detect, deliver, and assess methodology to direct friendly forces to attack the right target with the right asset at the right time. The targeting working group provides the HPTL to the operations, intelligence, and fires support element. The staff employs the HPTL to understand and determine attack guidance and to refine the collection plan. This list may also indicate the commander's operational need for battle damage assessment of the specific target and the time window for collecting and reporting it (ATP 3-60).

The CEWO integrates EW into the targeting process. After the targeting board has approved an EW target, the CEWO deconflicts the EW activity with the friendly use of the EMS. To support targeting, the CEWO—

- Matches EW resources with specific high-payoff targets and high-value targets.
- Ensures EW activities meet targeting objectives.
- Synchronizes EA with friendly use of the EMS.
- Coordinates with the SIGINT staff to gain targeting information that supports ES and EA.
- Provides EW mission management through the command post or joint operations center and the tactical air control party for airborne EA.
- Provides EW mission management as the EW control authority for ground or airborne EA when designated.
- Requests theater EW support.

*See pp. 4-29 to 4-34 for further discussion of targeting.*

## Joint Restricted Frequency List (JRFL)

The JRFL includes—

### Taboo Frequencies

Taboo frequencies are friendly frequencies of such importance that must never be deliberately jammed or interfered with by friendly forces. Normally these include international distress, safety, and controller frequencies. They are generally long-standing frequencies, taboo frequencies may be time-oriented, and the restrictions may be removed as the combat or exercise situation changes. During crisis or hostilities, short duration EA may be authorized on taboo frequencies for self-protection to provide coverage from unknown threats or threats operating outside their known frequency ranges, or for other reasons. *For more information about guarded, protected and taboo frequencies, refer to JP 3-13.1.*

### Protected Frequencies

Protected frequencies are friendly frequencies used for a particular operation, identified and protected to prevent them from inadvertent jamming by friendly forces while executing active EW operations against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless absolutely necessary or until coordination with the engaged unit is made. They are generally time-oriented and may change with the tactical situation. It is important to update protected frequencies periodically.

### Guarded Frequencies

Guarded frequencies are adversary frequencies currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the list changes as the adversary assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of the technical information.

## C. Staff Judge Advocate

Conducting EW requires an understanding of the ROE and legal authorities. The CEWO consults the SJA for the standing ROE and interpretation. The SJA or representative reviews EW activities to ensure compliance with existing DOD directives and instructions, ROE, and applicable domestic and international laws, including the law of armed conflict.

When considering EA or ES, the SJA will assist in the planning of operations and will review past operations. As part of the assistance, the SJA considers what impacts operations may have on host nation communications and legal implications related to the impacts.

# III. Electronic Warfare Configurations

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 3-6 to 3-8.

EW equipment requires configuration for successful deployment. Units use EW equipment in man-pack, vehicle, fixed-site, and airborne configurations. Equipment configuration includes—

- Choosing omnidirectional or directional antennas.
- The physical placement of equipment.
- Selecting power resources for EW equipment.
- Primary, alternate, contingency, and emergency (PACE) plan for tasking and reporting.

Power sources for EW equipment include—

- Power generators such as gasoline or diesel powered engines.
- Batteries for man packs and vehicle-mounted configurations.
- Shore power for fixed EW assets.

## Manpack Configuration

Manpack configurations include EA and ES capabilities. For manpack configurations, the CEWO considers the following—

- Limited available transmit power for EA.
- Weight of antennas and batteries carried by the Soldier.

## Vehicle-Mounted Configuration

Vehicle-mounted EW equipment supports units with EA and ES capabilities. Units use vehicle-mounted EW equipment during maneuver or at the halt. Vehicle-mounted configurations include—

- Mounted and dismounted configurations.
- Jamming capabilities.
- Direction finding (DF) capabilities for locating and targeting threat transmitters.
- PACE plan for tasking and reporting

## Fixed-Site Configuration

Fixed-site EW configurations have more available transmitting power than manpack and vehicle EW configurations. Fixed EW configurations have multiple transmitters, receivers, and antennas that enable multiple EW activities to occur simultaneously. A fixed site may include transportable systems that require configuration and operation only at the halt requiring personnel to install or construct the system.

## Airborne Configuration

Airborne EW is the coupling of EW assets to airborne platforms such as unmanned aerial systems, tethered balloons, and rotary and fixed-wing aircraft. They provide an extended range over ground-based assets and greater mobility than ground-based assets. In addition, they support ground-based units.

The synchronization of airborne EW missions requires detailed planning. The time on target for airborne EW assets coupled to rotor and fixed-wing platforms is normally brief. Time on target for airborne EW is limited due to the high rate of speed of the aircraft. The short time on target is also a technique used to minimize the threat's abilities to detect the platforms using visual, DF and radar detection techniques.

# V. EW Employment Considerations

Ref: ATP 3-12.3, *Electronic Warfare Techniques* (Jul '19), pp. 3-5 to 3-6.

The CEWO analyzes the operation and EW employment considerations early in the MDMP. These considerations include—

- Survivability of personnel and equipment.
- The time required to build or improve the unit's EP posture and position EA and ES capabilities.
- Ability of EW resources to achieve the desired effects.
- Reprogramming of EW assets.
- Capabilities, limitations, advantages, and disadvantages of available EW and SIGINT assets equipped with ES capability.
- Intelligence available for targeting.

*Note. The G-2 (S-2) manages SIGINT resources that contribute to EW targeting.*

## Survivability

Survivability of personnel and equipment rely on force protection and EP techniques. EP enhances force protection efforts as another method to mitigate environmental and adversarial effects. The CEMA section plans the mitigation actions, and the commander decides what risk is acceptable for an EW mission. Force protection risk mitigating techniques include coordinating ground or air escort and configuring EW equipment with organic EP capabilities. EP is not force protection or self-protection. EP is an EMS-dependent system's use of electromagnetic energy and/or physical properties to preserve itself from direct or environmental effects of friendly and adversary EW, thereby allowing the system to continue operating (JP 3-13.1).

EP contributes to survivability. Antennas erected to minimum heights, while maintaining communications, prevent visual observation by the threat. This technique contributes to survivability. Survivability is a useful criterion for course of action analysis during the MDMP. For more information about EP, see chapter 7.

## Time

The CEWO uses available time to configure and position EW assets for optimal performance. Time also affects the selection of movement techniques for a mission. The CEWO synchronizes EA operations with maneuver and fire to maximize effects at the appropriate time. The CEWO also plans duration of EA effects based on target analysis to support survivability of EW assets.

## Efficacy

The CEWO considers which EW asset has the appropriate level of efficacy for an EW mission. Efficacy is the likelihood that an EW mission will achieve the desired effect. For example, EA has a minimum transmission power threshold. Transmission power settings below the threshold have reduced levels of efficacy to achieve the desired effect, whereas transmission power settings above the threshold have increased levels of efficacy to achieve the desired effect.

## Electronic Warfare Reprogramming

Electronic warfare reprogramming is the deliberate alteration or modification of electronic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment (JP 3-13.1). When information reveals that the adversary changes

frequencies for communications or there are other changes in the EME, the CEWO ensures the reprogramming of EW systems or target sensing systems, to include the employment technique. Reprogramming includes changes to defensive systems, software, firmware, hardware, and information collection systems (JP 3-13.1). The change in the EME may affect friendly communication systems also. The CEWO informs the spectrum manager of the changes to EW requirements to coordinate the adjustment in mission parameters and may recommend friendly communications frequency changes to the G-6 (S-6). The responsibility to reprogram EW equipment is the responsibility of the unit; however, units should be aware of reprogramming efforts when operating with multi-national forces. Reprogramming is a national responsibility due to the effect on the EME. Refer to JP 3-13.1 for more information about reprogramming. EW reprogramming examples include—

- Changing target frequencies for jamming as well as updating restricted frequencies.
- Changes location of sensors due to environmental changes or interference.
- Installing the latest available software, firmware, and hardware for EW and SIGINT equipment.

## Electronic Warfare Visualization

The CEMA section visualizes and simulates the EMS, manmade effects, and environmental impacts. The information the section gains informs friendly actions and may provide insight to possible enemy COAs. There are automated tools to assist the CEMA section with the following tasks:

- Providing input to the common operational picture.
- Displaying sensor information from EW and SIGINT assets including—
- Detecting emitters and plotting lines of bearing.
- Analyzing circular error probable ellipse.
- Conducting mission planning and rehearsals.
- Managing EW assets.
- Modeling and visualizing how the EME responds to friendly and enemy EW activities.

The CEMA section analyzes the EME using—

- EMS sensors.
- Threat system databases.
- Intelligence information.
- Operational environment factors.

EW personnel require updates as the situation changes. The tools combined with staff interaction and the command and control system provide the updates.

## VI. Electronic Warfare Assessment

EW assessment is continuously monitoring and evaluating the impact of EW on the current situation and the progress of an operation. CEWOs continually assess the current situation and progress of the operation and compare it with the concept of operations, mission, and commander's intent. Assessment occurs throughout planning, preparation, and execution; it includes three major tasks:

- Continuously identifying threat vulnerabilities and reactions to friendly EW activities.
- Continuously monitoring EW activities to ensure alignment with the commander's desired endstate.
- Evaluating the operation against measures of effectiveness and measures of performance and making necessary adjustments.

The targeting working group synchronizes EW effects with other effects. The CEWO coordinates and synchronizes joint and multinational air and ground EW capabilities. The CEWO also manages the organic EW activities within the main command post.

### Measures of Performance and Effectiveness (MOPs/MOE)

The CEWO develops the measures of performance and measures of effectiveness for evaluating EW activities during execution. Measures of effectiveness measure the degree to which an EW capability achieved the desired result. Normally, the CEWO measures this by analyzing data collected by both active and passive means.

Measures of effectiveness help define whether a unit is creating the desired effect(s) or conditions in an operational environment. Example questions to measure EW effectiveness include—

- Did the EA disrupt enemy radar assets?
- Is the enemy radar retuning?
- Is there increased radio traffic on the radar command and control network?

Measures of performance help evaluate whether a unit is accomplishing tasks to standard. In the context of EW, example questions of measures of performance include—

- Is the EA asset transmitting at the necessary power?
- Is the EA asset transmitting in the required bandwidth?
- Is the EA asset transmitting using the correct polarization?
- Are all assets for a given mission operating in proper synchronization?

CEWOs use caution when selecting measures of effectiveness to avoid flaws in an analysis of the EW mission. For example, the lack of enemy electronic activity, such as communications or improvised explosive device initiation, does not necessarily mean it was the result of the EW mission; other factors may be the cause. Another example of a flawed measure of effectiveness is the premature conclusion that an EA degraded or disrupted a radio communication that resulted in an enemy commander not being able to direct the maneuver of subordinate forces using a specific frequency during a battle engagement. The enemy commander may have an alternate means of communication.

Effective EW Planning continues during all phases of an operation. The planning of EW requires significant preparation to achieve successful execution of EW tasks. The CEWO uses assessment techniques to measure success.

# II(b). Electromagnetic Attack Request

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. E-9 to E-12. See also p. 3-25.

Typically, Army units at corps and below have the organic capabilities to conduct EW within their assigned AO. The joint force commander typically delegates electromagnetic attack control authority to subordinate commanders conducting EW missions within their assigned AO. Commanders must ensure EW has been integrated and synchronized across the staff and according to the higher commander's guidance parameters.

## I. Electromagnetic Attack Request

Dynamic targeting is targeting that prosecutes targets identified too late or not selected for action in time to be included in deliberate targeting. Dynamic targeting is normally employed in current operations planning because the nature and timeframe associated with current operations typically requires more immediate responsiveness than is achieved in deliberate targeting (JP 3-60). Dynamic targeting is used for targets of opportunity that includes unscheduled targets and unanticipated targets. When immediate airborne EA is required for deliberate targeting, for example, when a ground maneuver unit requires jamming enemy communications before engagement, a unit can request support using an EA request. Units also submit an EA request for EA support when a mission cannot pre-plan due to some operations' immediate nature. The EA request prepares the aircrew providing EA support (see ATP 3-09.32). The JTF headquarters, the joint force land component command, the joint force air component command, and the air operations center must collaboratively plan airborne EA before an operation. This planning and coordination provides the joint force air component command the necessary time to identify and prepare an electronic combat squadron that will remain on standby throughout the mission.

Electromagnetic Attack Request	
Do not transmit line numbers. Units of measure are standard unless briefed.	
Lines 1,2 and 4 are mandatory readback (*). Jam Control Authority (JTAC) may request additional readback.	
JCA; " _____ Foxfire 06 _____, this is _____ Forward 09 _____," (aircraft call sign) (JTAC call sign)	
1. Target/ or Effect Description: " _____ Disrupt _____,"	
a. Rapper or Target Name      radio transmitter	
b. Frequency (if known)      107.1 MHZ	
c. Modulation                  FM	
2. Target Location; " _____ N 46° 41' 33.228" W 120° 947.2322" _____," (latitude and longitude or MGRS)	
3. Remarks: " _____ to current remarks or special instructions _____,"	
<b>Legend</b> JTAC    joint terminal attack controller      N    North MGRS    military grid reference system      W    West	

Ref: FM 3-12 (Aug '21), fig. E-5. *Electromagnetic attack request.*



## Planning (Cyber & EW)

# III. Targeting (D3A)

*Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), pp. 4-11 to 4-17.*

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). A target is an entity or object that performs a function for the adversary considered for possible engagement or other actions. (JP 3-60).

When targeting for cyberspace effects, the physical network layer is the medium through which all digital data travels. The physical network layer includes wired (land and undersea cable), and wireless (radio, radio-relay, cellular, satellite) transmission means. The physical network layer is a point of reference used during targeting to determine the geographic location of an enemy's cyberspace and EMS capabilities.

When targeting, planners may know the logical location of some targets without knowing their physical location. The same is true when defending against threats in cyberspace. Defenders may know the logical point of origin for a threat without necessarily knowing the physical location of that threat. Engagement of logical network layer targets can only occur with a cyberspace capability.

The logical network layer provides target planners with an alternate view of the target that is different from the physical network layer. A target's position in the logical layer is identified by its IP addresses. Targets located by their IP address depict how nodes in the physical layer correlate to form networks in cyberspace. Targeting in the logical layer requires the IP address and access to the logical network to deliver cyberspace effects. The ability of adversaries to change logical layer network configurations can complicate fires and effects against both logical and cyber-persona layer targets, but the operational benefit of affecting those targets often outweigh targeting challenges.

The inability to target a cyber-persona in a distinct area or form in the physical and logical network layers presents unique complexities. Because of these complexities, target positioning at the cyber-persona layer often requires multiple intelligence collection methods and an extensive analysis to develop insight and situational understanding to identify actionable targets. Like the logical network layer, cyber-personas can change quickly compared to changes in the physical network layer.

Electromagnetic Attack (EA) is exceptionally well suited to attack spectrum-dependent targets that are difficult to locate physically, cannot be accurately targeted for lethal fires, or require only temporary disruption. The fires support element plans, prepares, executes, and assesses fires supporting current and future operations by integrating coordinated lethal and nonlethal effects through the targeting process. Lethal and nonlethal effects include indirect fires, air and missile defense, joint fires, cyberspace attacks, and EA.





Targeting is a multidiscipline effort that requires coordinated interaction among the commander, the fires support element, and several staff sections that form the targeting working group. The commander prioritizes fires to the targeting working group and provides clear and concise guidance on effects expected from all fires, including cyberspace attacks and EA. Priority of fires is the commander's guidance to the staff, subordinate commanders, fires planners, and supporting agencies to employ fires in accordance with the relative importance of the unit's mission (FM 3-09). The targeting working group determines which targets to engage and how, where, and when to engage them based on the targeting guidance and priorities of the commander.

The targeting working group assigns lethal and nonlethal capabilities, including cyberspace attack and EA capabilities, to produce the desired effect on each target, ensuring compliance with the rules of engagement. The CEMA section participates in the targeting working group and provides recommendations for the employment of cyberspace and EMS-related actions against targets to meet the commander's intent and inclusion in the scheme of fires. Scheme of fires is the detailed, logical sequence of targets and fire support events to find and engage targets to accomplish the supported commander's objectives (JP 3-09).

The CEMA section works closely with the fires support element to coordinate and manage cyberspace and EW assets as part of the fire support plan. This process is called fire support coordination and is the planning and executing of fire so that targets are adequately covered by a suitable weapon or group of weapons (JP 3-09).

Targeting Functions

The G-2 or S-2, in collaboration with the CEMA section and the fires support element, detects, identifies, and locates targets through target acquisition. Effective employment of weapons, including EA and cyberspace attacks, require sufficient intelligence gained through target acquisition. The G-2 or S-2 conducts information collection to provide the fires support element, members of the targeting working group, and members of the targeting board with intelligence information used for targeting. This information includes threat cyberspace and EMS-enabled capabilities that require an individual or combined effect from lethal or nonlethal attacks.

Targeting Methodology			
 Decide	 Detect	 Deliver	 Assess
<ul style="list-style-type: none"><li>▪ Target Development</li><li>▪ TVA</li><li>▪ HPT and HVT</li><li>▪ TSS</li><li>▪ Attack Options</li><li>▪ Attack Guidance</li></ul>	<ul style="list-style-type: none"><li>▪ Target Deception Means</li><li>▪ Detection Procedures</li><li>▪ Target Tracking</li></ul>	<ul style="list-style-type: none"><li>▪ Attack</li><li>▪ Planned Targets</li><li>▪ Targets of Opportunity</li><li>▪ Desired Effects</li><li>▪ Attack Systems</li></ul>	<ul style="list-style-type: none"><li>▪ Tactical Level</li><li>▪ Operational Level</li><li>▪ Restrike</li><li>▪ Feedback</li></ul>

Ref: ADP 3-19, Fires (Jul '19) and ATP 3-60, Targeting (May '15).

Targeting occurs continuously throughout operations. Army targeting methodology consists of four functions: decide, detect, deliver, and assess (D3A). These targeting functions occur throughout the operations process. Commanders and staff should also be conversant with joint targeting methodology and understand how each of these processes and methodologies relate, because cyberspace operations and EW are usually coordinated by a joint force commander. Table 4-1, page 4-13, illustrates a crosswalk between the operations process, the joint targeting cycle, D3A, and military decision-making process.

# Targeting Crosswalk

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), table 4-1.

Operations Process		Joint Targeting Cycle	D3A	Military Decision-Making process	Targeting Tasks
Continuous Assessment	Plan	1. Commander's Objectives, Targeting Guidance, and Intent.	Decide	Mission Analysis	<ul style="list-style-type: none"><li>Perform target value analysis to develop fire support (including cyberspace, electromagnetic warfare, and information related capabilities) high-value targets.</li><li>Provide fire support, information-related capabilities, cyberspace, and electromagnetic warfare related input to the commander's targeting guidance and desired effects.</li></ul>
		2. Target Development and Prioritization.		Course of Action Development	<ul style="list-style-type: none"><li>Designate potential high-payoff targets.</li><li>Deconflict and coordinate potential high-payoff targets.</li><li>Develop a high-payoff target list.</li><li>Establish target selection standards.</li><li>Develop an attack guidance matrix.</li><li>Develop fire support, cyberspace, and electromagnetic warfare related tasks.</li><li>Develop associated measures of performance and measures of effectiveness.</li></ul>
		3. Capabilities Analysis.		Course of Action Analysis	<ul style="list-style-type: none"><li>Refine the high-payoff target list.</li><li>Refine the target selection standard.</li><li>Refine the attack guidance matrix.</li><li>Refine fire support tasks.</li><li>Refine associated measures of performance and measures of effectiveness.</li></ul>
		4. Commander's Decision and Force Assignment.		Orders Production	<ul style="list-style-type: none"><li>Finalize the high-payoff target list.</li><li>Finalize target selection standards.</li><li>Finalize the attack guidance matrix.</li><li>Finalize the targeting synchronization matrix.</li><li>Finalize fire support tasks.</li><li>Finalize associated measures of performance and measures of effectiveness.</li><li>Submit information requirements to battalion or brigade G-2/S-2.</li></ul>
	Prepare	5. Mission Planning and Force Execution.	Detect		<ul style="list-style-type: none"><li>Execute Information Collection Plan.</li><li>Update information requirements as they are answered.</li><li>Update the high-payoff target list, attack guidance matrix, and targeting synchronization matrix.</li><li>Update fire support, cyberspace, and electromagnetic warfare related tasks.</li><li>Update associated measures of performance and measures of effectiveness</li></ul>
	Execute	6. Assessment	Deliver		<ul style="list-style-type: none"><li>Execute fire support, cyberspace attacks, and electromagnetic attacks according to the attack guidance matrix and the targeting synchronization matrix.</li></ul>
	Assess		Assess	<ul style="list-style-type: none"><li>Assess task accomplishment (as determined by measures of performance).</li><li>Assess effects (as determined by measures of effectiveness).</li><li>Refine fire support tasks and associated measures and reengage target if required</li></ul>	
	Legend: D3A     decide, detect, deliver, and assess				

Planning  
(Cyber & EW)

# I. Decide

The decide function is the first step of the targeting process. It begins with the military decision-making process and continues throughout an operation. The CEMA section conducts the following actions during the decide function of targeting—

- Threat cyberspace and EW-related capabilities and characteristics during target value analysis to identify high-value targets. A high-value target is a target the enemy commander requires for the successful completion of the mission (JP 3-60).
- Identifying potential cyberspace and EW-related HPTs. A high-payoff target is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (JP 3-60). A high-payoff target is a high-value target that must be acquired and successfully engaged for the success of the commander's mission.
- Specific targets that should be acquired and engaged using a cyberspace attack or EA capability and established target selection standards.
- Location and time that targets are likely to be found through intelligence operations and how long the target will remain fixed.
- Surveillance, reconnaissance, and target acquisition objectives for targets receiving cyberspace attacks or EA and determining if the unit has the necessary cyberspace attack or EA capabilities to deliver appropriate effects.
- Cyberspace and EMS-related IRs essential to the targeting effort.
- When, where, and with what priority should the targets be engaged, and what cyberspace attack or EA capability to employ for effects.
- The level of effectiveness that constitutes a successful cyberspace attack or EA and if the engagement achieved the commander's objective.
- If a cyberspace attack or EA can affect a target, and how and what type of cyberspace attack or EA can create the desired effect.
- How to obtain the information needed to assess a cyberspace attack or EA to determine success or failure, and who will receive and process it.
- Who will be the decision-making authority to determine the success or failure of a cyberspace attack or EA?
- What contingency action will occur if a cyberspace attack or EA is unsuccessful, and who has the authority to direct those actions?
- Identifying the unit's EW assets available for tasking and begin drafting FRAGOS.
- Drafting the RFS for OCO support to meet targeting requirements.
- Collaborating with units at higher, lower, and adjacent echelons for EW support to satisfy identified gaps in EW capabilities.
- Drafting the Joint Tactical Air Request for airborne EA and other necessary EW requesting forms, if required.
- Open communications with the higher command to receive updates on whether anticipated cyberspace attack and EA-related targets have been validated and added to the JTF headquarters' joint target list.
- Discussing cyberspace and EW-related risk that the commander will use to make risk determinations.
- Determining the level of authorities for the engaging targets using cyberspace and electromagnetic attacks.

During the decide function, the targeting working group identifies target restrictions that prohibit or restrict cyberspace attacks or EA on specified targets without approval from higher authorities. The sources of these restrictions include military risk, the law of war, rules of engagement, or other considerations. The JTF annotates entities within the AO prohibited from attack on the no-strike list and targets with restrictions on the restricted target list.

## II. Detect

The detect function of the targeting process is the second step of the targeting process; during this step ES capabilities or other target acquisition assets locate and track a specified target to the required level of accuracy in time and space. During the detect function, the G-2 or S-2 coordinates with the targeting working group in developing the information collection plan. Before conducting the deliver function, the targeting team must establish measures of performance and measures of effectiveness for cyberspace and electromagnetic attacks to ensure they meet the commander's objectives.

The targeting working group focuses on the surveillance effort by identifying named areas of interest and target areas of interest integrated into the information collection plan. Named areas of interest are typically selected to capture indications of adversary courses of action but may be related to conditions of the OE.

The targeting working group identifies HPTs during planning and war-gaming. Target areas of interest that require specific engagements using cyberspace attack or EA capabilities differ from engagement areas. An engagement area is an area of concentration where a commander employs all available weapons to engage a target. In contrast, a target area of interest engagement uses a specific weapons system to engage a target. During the detect function, the CEMA section conducts the following—

- Provides cyberspace and EW-related IRs to determine HPTs that, when validated by the commander, are added to the priority intelligence requirement.
- Tasks EW assets, when required, to conduct electromagnetic reconnaissance to support information collection.
- Updates cyberspace attack and EA-related HVTs and HPTs.
- Determines if identified targets can be affected using OCO or EA (or both), and what type of EA capability can create the desired effect

*Note. The CEMA section alone cannot determine the type of cyberspace attack capability to use on targets. The CEMA section must coordinate with higher headquarters CEMA staff and appropriate joint cyberspace entities to develop an understanding of availability, feasibility, and suitability of specific cyberspace capabilities.*

- Advocating for the nomination of cyberspace attack and EA-related targets to the JTF headquarters' joint integrated prioritized target list and the joint targeting cycle.
- Developing the RFS for OCO support.

## III. Deliver

The deliver function of the targeting process executes the target engagement guidance and supports the commander's battle plan upon confirmation of the location and identity of HPTs. Close coordination between the CEMA section, intelligence, and fires support element is critical when detecting targets and delivering cyberspace attacks and EA. The fire support coordinator or fire support officer details fires coordination in the OPLAN or OPORD or target synchronization matrix.

## IV. Assess

The assess function occurs throughout the operations process. During the assess function, targets are continuously refined and adjusted by the commander and staff in response to new or unforeseen situations presented during operations. Combat assessment measures the effectiveness of cyberspace attack and EA capabilities on the target and concludes with recommendations for reattack, continued attack, or to cease an attack. Recommendations for reattack, continued attack, and ceasing EA are combined G-3 or S-3 and intelligence functions approved by the commander.

*For more information on the targeting cycle and target development process, refer to ATP 3-60.*

# Considerations When Targeting

Ref: FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21), pp. 4-16 to 4-17.

The fires support element, in collaboration with the G-3 or S-3 and G-2 or S-2, uses targeting cycles and target development processes to select, prioritize, determine the type of effects, and duration of effects on targets. CEMA's planning, integrating, synchronizing, and assessing cyberspace operations and EW becomes apparent during the targeting process.

## Characteristics of Cyberspace and EW Capabilities

Cyberspace capabilities are developed based on gathered intelligence and from operational and mission variables attained regarding an OE. In cyberspace operations, cyberspace forces consider such conditions as the type of computer operating system used by an enemy or adversary, the make and model of the hardware, the version of software installed on an enemy or adversary's computer, and the availability of cyberspace attack resources before creating effects on a target. EW capabilities are also developed based on gathered intelligence on operational and mission variables attained regarding an EMOE. In EW, targeting planners compare the types and capabilities of known spectrum-dependent devices that enemies use to the availability of EW resources before creating EW effects on a target. Targets include enemy spectrum-dependent devices carried by personnel and spectrum dependent systems used with or in weapons systems, sensory systems, facilities, and cyberspace capabilities that require the use of the EMS.

## Cascading, Compounding, and Collateral Effects

The CEMA section should understand the overlaps amongst the military, other government, corporations, and private sectors in cyberspace. These overlaps are particularly important for estimates of possible cascading, compounding, or collateral effects when targeting enemy and adversary cyberspace capabilities. The same level of consideration is required when targeting enemy and adversary spectrum-dependent devices in the EMS.

Cyberspace capabilities can create effects beyond the geographic boundaries of an AO and a commander's area of interest. Employing cyberspace capabilities for attack or manipulation purposes within an area of interest require additional authorities beyond those given to a corps and below commander. Effects resulting from cyberspace attack operations can cause cascading effects beyond the targeted system that were not evident to the targeting planners. Cascading effects can sometimes travel through subordinate systems to attain access to the targeted system. Cascading effects can also travel through lateral or high-level systems to access a targeted system. Compounding effects are a gathering of various cyberspace effects that have interacted in ways that may have been either intended or unforeseen. Effects resulting from EA can cause cascading effects in the EMS beyond enemy or adversary's spectrum-dependent devices, disrupting or denying friendly forces access to the EMS throughout the EMOE. Collateral effects, including collateral damage, are the accidental cyberspace or EW effects of military operations on non-combatant and civilian cyberspace or EW capabilities that were not the intended target when implementing fires.

## Reversibility of Effects

Targeting planners must consider the level of control that they can exercise throughout each cyberspace and electromagnetic attack. Categorization of reversibility of effects are—

- **Operator reversible effects.** These effects can be recalled, recovered, or terminated by friendly forces. Operator reversible effects typically represent a lower risk of undesired consequences, including discovery or retaliation.
- **Non-operator reversible effects.** These are effects that targeting planners cannot recall, recover, or terminate after execution. Non-operator reversible effects typically represent a higher risk of response from the threat or undesired consequences.



# IV. Cyberspace (CEMA) in Operations Orders

*Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), pp. A-14 to A-15.*

OPLANs, OPORDs, FRAGORDs, and WARNORDs include cyberspace operations and EW information in various paragraphs and Annex C and Annex H. In OPLANs, OPORDs, and FRAGORDs, the scheme of CEMA is discussed in paragraphs 3.g. (Cyberspace Electromagnetic Activities); and 5.g. (Signal). In WARNORDs, cyberspace operations and EW information are in paragraph 5.g. (Signal).

Note. Paragraph 5g (Signal) has information regarding DODIN operations and spectrum management operations-related information.

Paragraph 3.g. (Cyberspace Electromagnetic Activities) describes how CEMA supports the concept of operations and refers the reader to Appendix 12 (Cyber Electromagnetic Activities) of Annex C (Operations) and Annex H (Signal) as required. Subdivision of Appendix 12 of Annex C and Annex H into the following cyberspace operations and EW-related information is as follows:

## ANNEX C—OPERATIONS (G-5 OR G-3 [S-3])

- Appendix 12—Cyberspace Electromagnetic Activities (Electronic Warfare Officer)
- Tab A—Offensive Cyberspace Operations
- Tab B—Defensive Cyberspace Operations (RA & IDM)
- Tab C—Electromagnetic Attack
- Tab D—Electromagnetic Protection
- Tab E—Electronic Support

## ANNEX H—SIGNAL (G-6 [S-6])

- Appendix 1—DODIN operations.
- Appendix 2—Voice, Video, and Data Network Diagrams.
- Appendix 3—Satellite Communications.
- Appendix 4—Foreign Data Exchanges.
- Appendix 5—Spectrum Management Operations (CEMA assisted).
- Appendix 6—Information Services.

## Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) to Operations Plans and Orders

Appendix 12 to Annex C of OPLANs or OPORDs describes the cyberspace operations and EW divisions (EA, EP, and ES) supporting the commander's concept of operations. The CEWO is overall responsible for publishing Appendix 12 of Annex C and oversees the CEMA section in assisting the G-6 or S-2 with the development of Appendixes 1 and 6 of Annex H. Appendix 12 of Annex C describes the scheme of cyberspace operations and EW and CEMA integration and synchronization processes. It also includes cyberspace operations and EW-related constraints from higher headquarters.

*See following pages (pp. 4-36 to 4-40) for a sample format for App. 12 to Annex C.*

# Appendix 12 to Annex C (Sample Format)

Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), p. A-16 to A-20.

## [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. Refer to 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 headquarter] [(classification of title)]

(U) **References:** Add any specific references to cyberspace electromagnetic activities, if needed.

1. (U) **Situation.** Include information affecting cyberspace and electronic warfare (EW) operations 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 (EMS); cyberspace may expand the area of local interest to a worldwide interest.

b. (U) **Area of Operations.** Include information affecting cyberspace and the EMS; cyberspace may expand the area of operations 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' cyberspace electromagnetic activities (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 EMS vulnerabilities. Identify friendly foreign forces with which subordinate commanders may operate. Identify potential conflicts within the EMS, 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 area of operations that may impact cyberspace and EW operations or implementation of cyberspace and EW operations specific equipment and tactics. See Annex V (Interagency) as required.

[page number]

[CLASSIFICATION]

[CLASSIFICATION]

f. (U) Third Party. Identify and describe other organizations, both local and external to the area of operations that have the ability to 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.

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.

1. (U) Mission. State the commander's mission and describe cyberspace and EW operations to support the base plan or order.

2. (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 section, elements, and working groups outside the CEMA section and working group. Describe the plan for the integration of unified action 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 operational 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 unified action 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. or allied or multinational networks or information), and possible conflicts. Describe actions that will prevent enemy and adversary action(s) to critically degrade the unified command's ability to effectively conduct military operations in its area of operations. 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

[page number]

[CLASSIFICATION]

Continued on next page

Continued on next page

Planning  
(Cyber & EW)

[Classification]

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 (DCO). Synchronize the CEMA section with the IO officer. Pass requests for offensive cyberspace operations (OCO) to higher headquarters for approval and implementation. Describe how DOD information network operations support the commander's intent and concept of operations. Synchronize DODIN operations with the G-6 (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 network operations. (Reference appropriate annexes and appendixes as needed to reduce duplication).

(1) (U) DODIN Operations. Describe how information operations are coordinated, synchronized, and support operations integrated with the G-6 (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 DCO 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 OCO 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 OCO.

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 unified action partner EW capabilities which support the commander's intent and concept of operations. State the electromagnetic attack, electromagnetic protection, and electromagnetic warfare support measures and plan for integration. Identify target sets and effects, by priority, for EW operations. Synchronize with IO officer. See the following attachments as required: Tab C, D, E (Electromagnetic Warfare) to Appendix 12 (Cyberspace Electromagnetic Activities); Appendix 15 (Information Operations of Annex C).

(1) (U) Electromagnetic Attack. Describe how offensive EW 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 defensive EW activities are coordinated, synchronized, and support operations. See Tab D (Electromagnetic Protection) to Appendix 12 (Cyberspace Electromagnetic Activities).

(3) (U) Electromagnetic Warfare Support. Describe how EW support activities are coordinated, synchronized, and support operations. See Tab E (Electromagnetic Warfare 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 achieve 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. Describe the plan for the integration of unified action partners' spectrum management operations capabilities. 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.

[page number]

[CLASSIFICATION]

Continued from previous page

Continued from previous page

[Classification]

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.

**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 (CPs), including the location of each CP and its time of opening and closing.

(2) (U) Reports. List cyberspace and EW operations specific reports not covered in SOPs. See Annex R (Reports) as required.

c. (U) Signal. Address any cyberspace and EW operations 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]

*Use only if the commander does not sign the original attachment. If the commander signs the original, no further authentication is required. If the commander does not sign, the signature of the preparing staff officer requires authentication and only the last name and rank of the commander appear in the signature block.*

[page number]

[CLASSIFICATION]

Continued on next page

Planning  
(Cyber & EW)

Continued on next page

[Classification]

**ATTACHMENTS:** *List lower level attachment (tabs and exhibits). If a particular attachment is not used, place "not used" beside the attachment number. Unit standard operating procedures will dictate attachment development and format. Common attachments include the following:*

**APPENDIX 12 (CYBERSPACE ELECTROMAGNETIC ACTIVITIES) TO ANNEX C (OPERATIONS) TO OPERATION PLAN/ORDER** [number] [(code name)]-[issuing headquarter] [(classification of title)]

**ATTACHMENT:** *List lower-level attachment (tabs and exhibits)*

Tab A -Offensive Cyberspace Operations

Tab B -Defensive Cyberspace Operations-Response Actions

Tab C -Electromagnetic Attack

Tab D -Electromagnetic Protection

Tab E -Electromagnetic Support

**DISTRIBUTION:** *Show only if distributed separately from the base order or higher-level attachments.*

[page number]

[CLASSIFICATION]

Continued from previous page

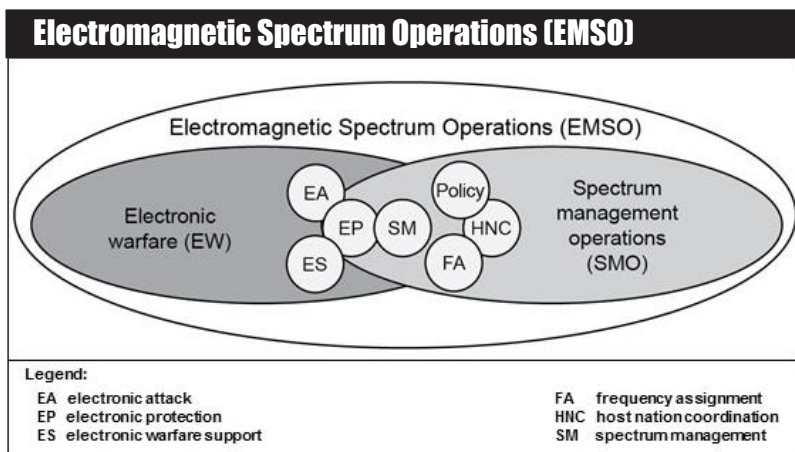
Continued from previous page

# I. Spectrum Management Operations (SMO/JEMSO)

Ref: FM 3-12, *Cyberspace & Electronic Warfare Operations* (Apr '17), pp. 1-25 & 1-34; JP 3-85, *Joint Electromagnetic Spectrum Management Operations* (May '20); and ATP 6-02.70, *Techniques for Spectrum Management Operations* (Oct '19).

## I. Electromagnetic Spectrum Operations (EMSO)

Electromagnetic Spectrum Operations (EMSO) are comprised of electronic warfare (EW) and spectrum management operations (SMO). The importance of the EMS and its relationship to the operational capabilities of the Army is the focus of EMSO. EMSO include all activities in military operations to successfully control the EMS. Figure 1-8 illustrates EMSO and how they relate to SMO and EW.



Ref: FM 3-12, *Cyberspace & Electronic Warfare Operations* (Apr '17), figure 1-8. *Electromagnetic spectrum operations. See also chap. 3, Electronic Warfare.*

### Spectrum Management Operations (Army) See p. 5-4.

Spectrum Management Operations (SMO) consists of the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment (EMOE), during all phases of military operations (FM 6-02).

### Joint Electromagnetic Spectrum Operations (JEMSO) See p. 5-5.

JEMSO are military actions undertaken by a joint force to exploit, attack, protect, and manage the EMOE. These actions include/impact all joint force transmissions and receptions of electromagnetic (EM) energy. JEMSO are offensively and defensively employed to achieve unity of effort and the commander's objectives. JEMSO integrate and synchronize electromagnetic warfare (EW), EMS management, and intelligence, as well as other mission areas, to achieve EMS superiority.

See following pages (pp. 5-2 to 5-3 ) for an overview and discussion of the electromagnetic operational environment (EMOE).

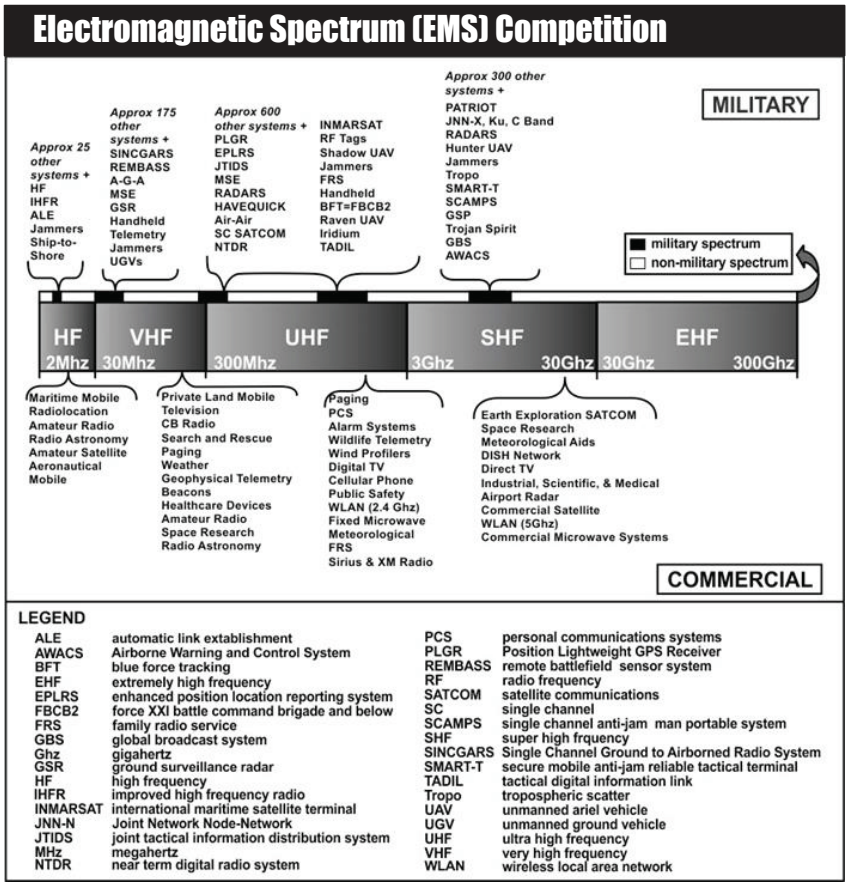


# Electromagnetic Operational Environment (EMOE)

Ref: JP 3-85, Joint Electromagnetic Spectrum Management Operations (May '20); pp. 1-2 to 1-3.

## Electromagnetic Spectrum (EMS)

The EMS is a maneuver space consisting of all frequencies of EM radiation (oscillating electric and magnetic fields characterized by frequency and wavelength). The EMS is often organized by frequency bands, based on certain physical characteristics. The EMS includes radio waves, microwaves, infrared (IR) radiation, visible light, ultraviolet radiation, x-rays, and gamma rays.



Ref: ATP 6-02.70, Techniques for Spectrum Management Operations (Oct '19), fig. 1-3. Electromagnetic spectrum competition.

## Electromagnetic Environment (EME)

The EME is the actual EM radiation encountered in a particular operational area (OA). The EME is the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted EM emission levels encountered by a military force, system, or platform when performing its mission in its intended OE. It is important to note that not all EM radiation encountered by joint forces will impact operations.



# Electromagnetic Operational Environment (EMOE)

The EMOE is a composite of the actual and potential EM radiation, conditions, circumstances, and influences that affect the employment of capabilities and the decisions of the commander. It includes the existing background radiation (i.e., EME) as well as the friendly, neutral, adversary, and enemy EM systems able to radiate within the EM area of influence. This includes systems currently radiating or receiving, or those that may radiate, that can potentially affect joint operations.

The EMOE has the following attributes:

**Physical.** The EMOE is part of the physical environment. EM radiation is a physical phenomenon. Both natural and manmade factors (e.g., terrain, weather, atmospheric conditions, sea state, transmitters, power lines, static electricity) influence EM radiation and the organizations and systems that employ it. Military forces maneuver through all environments, including the EMOE, to gain positions of advantage over adversaries and enemies. EMOE maneuver requires effective management of spectrum occupancy.

**Pervasive.** The EMS permeates all parts of the OE. Military forces use the EMOE to integrate, synchronize, and otherwise enhance their operations. The critical dependencies of modern military operations on EMS activities, coupled with the wide range of effects that can be created through electromagnetic spectrum operations (EMSO), are a potent force multiplier.

**Constrained.** Although the EMS contains an unlimited number of frequencies, its use for military purposes is limited by physics, policy, and current technology. EM radiation has unique physical properties that dictate its use (e.g., short- or long-range communications, sensing). Additionally, use of the EMS is subject to international treaties and laws, as well as nation-state laws and regulations. Technology bounds those portions of the EMS that are accessible and exploitable (i.e., advances in technological capabilities will result in expanded use of the EMS).

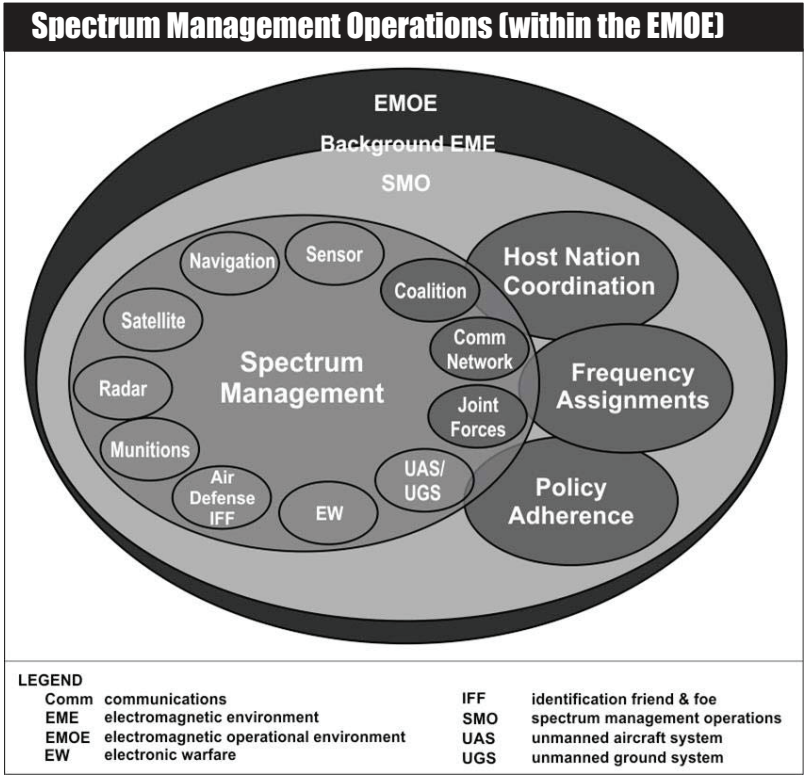
**Congested.** The EMOE encountered by joint forces is congested due to military and nonmilitary use, resulting in a commensurate increase in the number and density of EM emitters. As a result of physical characteristics and technology, civilian and military organizations increasingly seek to transmit and receive EM energy in the same or adjacent spectral bands. For instance, myriad stakeholders (e.g., cell phone and wireless Internet providers, media) continue to expand their EMS bandwidth requirements, reducing the open EM areas conducive to joint force maneuver. This congestion leads to electromagnetic interference (EMI) to a receiver. EMI is any EM disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of EMS-dependent systems, electronics, and electrical equipment.

**Contested.** Since modern military operations are critically dependent on the EMS, a key goal of our adversaries and enemies is to deny our ability to use it successfully. For example: antiradiation missiles and other destructive weapons are used to degrade or destroy transmitters and receivers, while EM energy can be used to disrupt or degrade a receiver's operation.

**Dynamic.** The EMOE experienced by the joint force is continuously changing, as existing systems are modified, new systems are deployed, units change locations, threats transmit, or natural phenomena occur. Since EM energy travels at the speed of light, military activities in the EMS may provide a decisive advantage by enabling commanders to make decisions, conduct operations, and create effects more rapidly than the threat. Agility in spectrum operations provides joint force operations the flexibility and adaptability to achieve mission success in dynamic EMOEs.

## II. Spectrum Management Operations (SMO)

Spectrum management operations (SMO) consists of the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment (EMOE), during all phases of military operations (FM 6-02). SMO includes all activities in military operations to manage the electromagnetic spectrum. SMO is the management function of electromagnetic spectrum operations (EMSO). SMO aim to manage resources within the EMOE while resolving electromagnetic interference (EMI) by conducting EMI analysis and resolution activities. Figure 1-1 depicts the various responsibilities related to spectrum management operations as they pertain to the EMOE.



Ref: ATP 6-02.70, *Techniques for Spectrum Management Operations* (Oct '19), fig.1-1. *Spectrum management operations within the EMOE.*

Spectrum managers coordinate and collaborate with spectrum managers working in joint environments. Collaboration with joint personnel and coalition partners is common practice necessary for the Army spectrum manager while using the highly saturated and limited spectrum available. In the joint environment, joint electromagnetic spectrum operations encompass joint electromagnetic spectrum management operations and electronic warfare with the same intent as the Army's electromagnetic spectrum operations.

See pp. 5-9 to 5-14 for further discussion of spectrum management operations.

## A. Objective of Spectrum Management Operations

SMO aims to ensure access to the electromagnetic spectrum in support of the Army's operational missions. SMO is a supporting function or enabler for unified land operations. SMO is an enabler for cyberspace electromagnetic activities (CEMA). Spectrum management is the operational, engineering, and administrative procedures to plan, coordinate, and manage use of the EMS and enables cyberspace, signal and electronic warfare (EW) operations.

SMO enables management of allotted and limited frequencies directly supporting operational forces throughout the world. The Army is dependent upon the use of the electromagnetic spectrum at all levels of unified land operations. An effective SMO program enables electronic systems to perform their functions in the intended environment without causing EMI.

Commanders must have the ability to see the use of their assigned spectrum resources so they can apply precise command and control (C2). The electromagnetic spectrum is a vital warfighting resource that requires the same planning and management as other critical resources such as fuel, water, and ammunition. Spectrum managers, with the appropriate expertise and tools, ensure that commanders have adequate knowledge of the utilization of the frequency spectrum to make decisions that positively influence the accomplishment of their missions.

## B. Spectrum Management Operations Core Functions

SMO core functions determine the tasks and requirements of the spectrum manager. These four functions are—

- Spectrum management.
- Frequency assignment.
- Host nation coordination.
- Policy adherence.

*See pp. 2-13 for further discussion of the EMS and SMO from FM 3-12. For more information on Army SMO, refer to FM 6-02 and ATP 6-02.70.*

## III. Joint Electromagnetic Spectrum Operations (JEMSO)

JEMSO are military actions undertaken by a joint force to exploit, attack, protect, and manage the EMOE. These actions include/impact all joint force transmissions and receptions of electromagnetic (EM) energy. JEMSO are offensively and defensively employed to achieve unity of effort and the commander's objectives. JEMSO integrate and synchronize electromagnetic warfare (EW), EMS management, and intelligence, as well as other mission areas, to achieve EMS superiority.

JEMSO support military operations throughout the competition continuum to achieve desired objectives and attain end states. During peacetime, JEMSO are conducted to ensure adequate access to the EMS and may include deconflicting use of the EMS between joint users and coordinating with a host nation (HN). As a crisis escalates toward armed conflict, JEMSO shift from EMS access coordination to EMS superiority, with coordinated military actions executed to exploit, attack, protect, and manage the electromagnetic operational environment (EMOE).

*See pp. 5-15 to 5-28 for discussion of planning joint electromagnetic spectrum operations (JEMSO).*

# A. JEMSO Actions

Ref: JP 3-85, *Joint Electromagnetic Spectrum Management Operations* (May '20); pp. 1-2 to 1-3.

JEMSO actions to exploit, attack, protect, and manage the EMOE rely on personnel and systems from EW, EMS management, intelligence, space, and cyberspace mission areas. Instead of these mission areas being planned and executed in a minimally coordinated and stovepiped fashion, JEMSO guidance and processes prioritize, integrate, synchronize, and deconflict all joint force operations in the EMOE, enhancing unity of effort. The result is a fully integrated scheme of maneuver in the EMOE to achieve EMS superiority and joint force commander (JFC) objectives.

## Exploitation

Exploitation takes full advantage of available information for tactical, operational, or strategic purposes. In a JEMSO context, exploitation refers to EMS systems capable of sensing the EMOE. Sensing systems support intelligence collection, SA, targeting, and warning. EMS sensors can be active (e.g., air-to-air radars, IFF interrogators) or passive (e.g., radar warning receivers, passive radars, IR weapons seekers). These sensing missions are typically executed through signals intelligence (SIGINT) and electromagnetic support (ES) operations.

## Electromagnetic Attack (EA)

JEMSO capabilities can directly produce effects in the EMOE. These capabilities can be used to deny (i.e., disrupt, degrade, destroy) and/or deceive an enemy's military EMS activities. EA is the division of EW involving the use of EM energy, including DE or antiradiation weapons, to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Typical EA capabilities include EM jamming and intrusion. EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EMS, to degrade or neutralize the enemy's combat capability. EM intrusion involves the intentional insertion of EM energy into transmission paths to deceive or confuse enemy forces. EA can be either active (i.e., radiating) or passive (i.e., non-radiating/reradiating). Examples of active EA systems (to include lethal and nonlethal DE) include lasers, electro-optical, IR, and RF weapons such as high-power microwave (HPM) or those employing an electromagnetic pulse (EMP). Examples of passive EA systems are chaff and corner reflectors. EA can also be used for offensive and defensive purposes.

- **Offensive EA.** Offensive EA describes the use of EA to project power in support of operations within the time and tempo of the scheme of maneuver. JEMSO planners use JFC guidance to integrate EA during joint planning through the joint planning group or operational planning group, coordinating effects and incorporating risk mitigation techniques to reduce collateral damage. In many cases, these activities suppress a threat for only a limited period of time. Examples include employing self-propelled decoys; jamming radar or C2 systems; using antiradiation missiles to suppress air defenses; using EM deception techniques to confuse intelligence, surveillance, and reconnaissance (ISR) systems; and using DE weapons to disable personnel, facilities, or equipment and disable or destroy materiel (e.g., satellites in orbit, airborne optical sensors, or massed land forces).
- **Defensive EA.** Defensive EA describes the use of EA to protect against threats by denying enemy use of the EMS to target, guide, and/or trigger weapons. EA used for defensive purposes in support of force protection or self-protection is often mistaken as EP. Although defensive EA actions and EP protect personnel, facilities, capabilities, and equipment, EP protects from the effects of EA or EMI, while defensive EA is primarily used to protect against lethal attacks by denying enemy use of the EMS to target, guide, and/or trigger weapons.

## Protect

As joint forces are critically dependent on exploiting the EMOE, JEMSO facilitate the necessary EMS access by minimizing EMI from friendly, neutral, adversary, and enemy actions. JEMSO integrate EW and EMS management protection actions throughout planning and execution, enabling joint force EMS-dependent systems to operate in the EMOE as intended. EP refers to the division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, adversary, or enemy use of the EMS, as well as naturally occurring phenomena that degrade, neutralize, or destroy friendly combat capability. EP focuses on system or process attributes or capabilities that eliminate or mitigate the impact of EMI. These inherent hardware features; processes; and dedicated tactics, techniques, and procedures (TTP) combine to enable friendly capabilities to continue to function as intended in contested and congested EMOEs.

## Manage

All joint force operations in the EMS must be managed to facilitate unity of effort in executing the planned scheme of maneuver within the EMOE. EMS management's objective is to enable EMS-dependent capabilities and systems to perform their functions as designed, without causing or suffering unacceptable EMI. EMS management provides the framework to utilize the EMS in the most effective and efficient manner. EMS management is analogous to the airspace management function in air operations, coordinating and integrating joint EMS use in terms of time, space, and frequency.

- **Electromagnetic Battle Management (EMBM).** EMBM includes actions to monitor, assess, plan, and direct operations in the EMS in support of the commander's objectives. It is the coordinated direction of all joint functions in the EMS to enable the orderly conduct of friendly EMSO. When exercised, EMBM is a commander's mechanism for informing all actions that shape the OE. EMBM is accomplished through an EMBM system that consists of the facilities, equipment, software, communications, procedures, and personnel essential for a commander to plan, direct, and control operations in the EMS.
- **Frequency Management (FM).** FM encompasses interference analysis and requesting, nominating, coordinating, assigning, and promulgating frequencies for EMS-dependent capabilities and systems. FM assigns frequencies for non-EA EM transmissions, conducts frequency deconfliction, and mitigates EMI. FM is a key component for developing EMS operating instructions and coordination measures. FM includes spectrum analysis, engineering, and assessment of EMS-dependent systems and developing EMS products such as the JRFL, joint communications-electronics operating instructions (JCEOI), and others, as required.
- **Host-Nation Coordination (HNC).** HNC is the coordination with nation states for authorization to operate EMS-dependent systems within national borders (includes use of systems that emanate across the border from other AOIs). Coordination is required when operating within foreign nations as well as the United States. Granting approval to transmit EM energy within a nation is a sovereign right. HNC is normally accomplished through procedures established by CCMD agreements with HNs.
- **Joint Spectrum Interference Resolution (JSIR).** A contested and congested EMS, coupled with dynamic military operations, makes encountering EMI in the EMOE very likely. In fact, most system degradation can be attributed to EMI. As such, JSIR identifies, reports, analyzes, and mitigates or resolves incidents of EMI. JSIR uses a continuous systematic process to report and diagnose the cause or source of EMI. CCMDs should ensure incidents of EMI are reported immediately and are resolved or mitigated. EMI can be induced intentionally, as in EA, or unintentionally, as a result of harmonics, spurious emissions, intermodulation products, improper operation, or inadequate EMS management.

## **B. Electromagnetic Environmental Effects (E3)**

*Ref: JP 3-85, Joint Electromagnetic Spectrum Management Operations (May '20); pp. I-11 to I-12.*

The impact of the EMOE upon the operational capability of military forces, equipment, systems, and platforms is referred to as electromagnetic environmental effects (E3).

Examples of E3 include electromagnetic compatibility (EMC), EMI, EMP, and EM radiation hazards. EM radiation hazards include hazards of electromagnetic radiation to personnel (HERP); hazards of electromagnetic radiation to ordnance (HERO); hazards of electromagnetic radiation to fuels (HERF); and natural phenomena effects such as space weather, lightning, and precipitation static.

### **HERP**

HERP is the potential hazard that exists when personnel are exposed to an EM field of sufficient intensity to heat the human body. Radar, communication systems, and EW systems which use high-power RF transmitters and high-gain antennas represent a biological hazard to personnel working on, or in the vicinity of, these systems. Therefore, stand-off areas around high-powered RF antennas should be clearly marked. Since it is not possible to visibly determine if an antenna is transmitting, personnel should avoid entering these stand-off areas at all times.

### **HERO**

HERO is the danger of accidental actuation of electro-explosive devices or otherwise electrically activating ordnance because of RF EM fields. This unintended actuation could have safety (premature firing) or reliability (dudding) consequences. HERO may be induced through holes or cracks in the casing, wires, or fuses and is most susceptible during assembly, disassembly, loading, or unloading.

### **HERF**

HERF is the potential hazard that is created when volatile combustibles, such as fuel, are exposed to EM fields of sufficient energy to cause ignition. HERF is most likely to occur when refueling operations are taking place. Care should be taken to separate fueling points and high-powered radar, radio, directed energy weapons, or jammers to reduce the possibility of RF induced arcs that could ignite fuel. Personnel must ensure proper grounding and static discharge procedures are adhered to and that RF transmissions be minimized or ceased during refueling operations.

### **Electromagnetic Pulse (EMP)**

The interaction of gamma radiation with the atmosphere can cause a short pulse of electric and magnetic fields that may damage and interfere with the operation of electrical and electronic equipment and can cause widespread disruption. EMP is one of the primary ways that a nuclear detonation produces its damaging effects. The effects of EMP can extend to hundreds of kilometers depending on the height and yield of a nuclear burst.

### **High-Altitude Electromagnetic Pulse (HEMP)**

A high-altitude electromagnetic pulse (HEMP) can generate significant disruptive field strengths over a continental-size area. The portion of the EMS most affected by EMP and HEMP is the radio spectrum. Planning for communication system protection is key when the potential for EMP is likely.

*For more information on E3, refer to Department of Defense Instruction (DODI) 3222.03, DOD Electromagnetic Environmental Effects (E3) Program.*

# II. Spectrum Management

*Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), pp. 1-34 to 1-35 and ATP 6-02.70, Techniques for Spectrum Management Operations (Oct '19), chap. 2.*

Spectrum management is the operational, engineering, and administrative procedures to plan, coordinate, and manage use of the electromagnetic spectrum and enables cyberspace, signal and EW operations. Spectrum management includes frequency management, host nation coordination, and joint spectrum interference resolution. Spectrum management enables spectrum-dependent capabilities and systems to function as designed without causing or suffering unacceptable electromagnetic interference. Spectrum management provides the framework to utilize the electromagnetic spectrum in the most effective and efficient manner through policy and procedure.

SMO are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. The SMO functional area is ultimately responsible for coordinating EMS access among civil, joint, and multinational partners throughout the operational environment. The conduct of SMO enables the commander's effective use of the EMS. The spectrum manager at the tactical level of command is the commander's principal advisor on all spectrum related matters.

The conduct of SMO enables and supports the execution of cyberspace operations and EW. SMO are critical to spectrum dependent devices such as air defense radars, navigation, sensors, EMS using munitions, manned and unmanned systems of all types (ground and air, radar, sensor), and all other systems that use the EMS. The overall objectives of SMO are to enable these systems to perform their functions in the intended environment without causing or suffering unacceptable electromagnetic interference. Understanding the SMO process in planning, managing, and employing EMS resources is a critical enabler for cyberspace and EW operations. SMO provides the resources necessary for the implementation of the wireless portion of net-centric warfare.

The spectrum manager should be an integral part of all electronic warfare (EW) planning. The SMO assists in the planning of EW operations by providing expertise on waveform propagation, signal, and radio frequency theory for the best employment of friendly communication systems to support the commander's objectives.

*See chap. 3, Electronic Warfare.*

## Frequency Interference Resolution

Interference is the radiation, emission, or indication of electromagnetic energy (either intentionally or unintentionally) causing degradation, disruption, or complete obstruction of the designated function of the electronic equipment affected. The reporting end user is responsible for assisting the spectrum manager in tracking, evaluating, and resolving interference. Interference resolution is performed by the spectrum manager at the echelon receiving the interference. The spectrum manager is the final authority for interference resolution. For interference affecting satellite communications, the Commander, Joint Functional Component Command for Space is the supported commander and final authority of satellite communications interference.



# I. Key SMO inputs to the MDMP

Ref: ATP 6-02.70, *Techniques for Spectrum Management Operations* (Oct '19), pp. 2-11 to 2-14.

Key inputs for the MDMP are actions, processes or information spectrum managers provide to the MDMP. SMO key outputs for MDMP are the completed CEOI, reports, frequency proposals or data call messages. Table 2-1 depicts the key SMO inputs and outputs for each step of the MDMP.

Key SMO inputs	Steps	Key SMO outputs
<ul style="list-style-type: none"> <li>Updated EMS database</li> <li>Unit electronic order of battle</li> <li>Library of EMS documents</li> <li>HN allocation tables</li> <li>Gather spectrum management tools</li> </ul>	<p><b>Step 1:</b> Receive Mission</p>	<ul style="list-style-type: none"> <li>Defined EMOE</li> <li>Data call message</li> <li>Identify EMS constraints</li> <li>JRFL guidance</li> </ul>
<ul style="list-style-type: none"> <li>Identified EMS capabilities pertaining to combat power</li> <li>List of unit's SSDs</li> <li>Frequency requests</li> <li>JRFL requests</li> </ul>	<p><b>Step 2:</b> Mission Analysis</p>	<ul style="list-style-type: none"> <li>Prioritized EMS use</li> <li>Completed JRFL</li> <li>Frequency reuse plans</li> <li>Initial EMS risk assessment</li> </ul>
<ul style="list-style-type: none"> <li>Commander's intent</li> <li>Frequency allotments</li> <li>Initial frequency assignments</li> <li>DD-1494 for unit's SDDs</li> </ul>	<p><b>Step 3:</b> Develop COA</p>	<ul style="list-style-type: none"> <li>M&amp;S of EMS to develop multiple COAs</li> <li>EMI/EW deconfliction</li> <li>Initial Spectrum Plan</li> <li>EMS COP</li> </ul>
<ul style="list-style-type: none"> <li>Initial Spectrum Plan</li> <li>Mitigating factors to decrease EMS risk</li> </ul>	<p><b>Step 4:</b> COA Analysis (War Game)</p>	<ul style="list-style-type: none"> <li>M&amp;S shows EMS advantages/disadvantages for each COA</li> <li>Continues analysis of EMS risk assessment</li> <li>Recommend modifications</li> </ul>
<ul style="list-style-type: none"> <li>Optional unit movement routes for planning COTM</li> <li>Refines EMS COAs</li> </ul>	<p><b>Step 5:</b> COA Comparison</p>	<ul style="list-style-type: none"> <li>M&amp;S depicts EMS use to compare COAs</li> <li>Recommended EMS COAs</li> </ul>
<ul style="list-style-type: none"> <li>Recommended EMS COA</li> <li>Coordinated frequency conflicts</li> <li>Frequency proposals</li> </ul>	<p><b>Step 6:</b> COA Approval</p>	<ul style="list-style-type: none"> <li>Commander selected EMS COA and any modifications</li> <li>Frequency assignments</li> </ul>
<ul style="list-style-type: none"> <li>Frequency assignments/allotments from higher echelon ESM</li> <li>HN frequency clearance</li> <li>CREW loadsets</li> </ul>	<p><b>Step 7:</b> Orders Production, Dissemination and Transition</p>	<ul style="list-style-type: none"> <li>The Spectrum Plan</li> <li>CEOI/JCEOI</li> <li>Annex H of OPORD</li> <li>Distribute frequency assignments to requestors</li> <li>CNR loadsets</li> </ul>

SMO supports the commander's SMO objectives during each step of the MDMP. The following are some responsibilities expected of the spectrum manager for each step—

## Step 1: Receipt of Mission

- The spectrum manager conducts data calls to attain a list of SDDs and their spectrum requirements.
- Using spectrum management tools, the spectrum manager models the operational area with digital topography and electromagnetic environmental effects information to analyze spectrum supportability.
- Using governmental and host nation spectrum allocation tables, the spectrum manager determines frequencies used in an AO.
- The spectrum manager compiles restrictions or constraints of spectrum use that may prevent planning and use of protected, taboo, and guarded frequencies in the AO. For a listing of the worldwide-restricted frequency list, see CJCSM 3320-01C.
- The spectrum manager should understand the EMOE for awareness of the spectrum occupancy in the AO. Colors representing users of the spectrum are—blue (friendly), red (enemy), and gray (neutral and civil).



## Step 2: Mission Analysis

- The spectrum manager analyzes the EMOE, highlighting unified action partners' spectrum users, and aid the commander in determining spectrum priorities.
- The spectrum manager conducts an initial spectrum risk assessment identifying the spectrum impact mission on unified action partners in the operational area. This process also identifies frequency usage conflicts such as EMI and frequency fratricide.
- The spectrum manager generates a frequency reuse plan for spectrum optimization and increased spectrum capabilities.
- The spectrum manager identifies spectrum constraints where certain frequencies are either taboo, protected, or guarded. Constraints include those frequencies not allocated for use by the host nation.
- The spectrum manager, with guidance from the CEWO, determines spectrum capabilities of combat power, such as EW and counter radio-controlled improvised explosive device electronic warfare (CREW) systems.

## Step 3: Course of Action Development

- Using spectrum management tools, the spectrum manager models the unit's boundaries and movement formations. The use of these models is for developing COA recommendations.
- Using spectrum management tools, the spectrum manager performs EMI and EW frequency deconfliction for both COA development and spectrum supportability.
- The spectrum manager generates frequency allotment and allocation tables for subordinate units.
- The spectrum manager identifies spectrum impact on civilian spectrum users in the AO.
- The spectrum manager evaluates primary, alternate, contingency, and emergency communications for each COA based on unit capabilities, software simulation, and spectrum supportability.

## Step 4: Course of Action Analysis (War Game)

- The spectrum manager identifies the spectrum advantages and disadvantages throughout the AO for each COA.
- The spectrum manager identifies mitigating factors for the spectrum risk assessment to reduce or eliminate risks.
- The spectrum manager recommends modifications to the COA based on newly identified spectrum requirements and supportability during the wargame.

## Step 5: Course of Action Comparison

- Using spectrum management tools, the spectrum manager develops multiple COAs. The commander determines the COA best suited for the mission.
- The spectrum manager analyzes routes used for movement of forces and advises the commander on routes with the least likelihood of spectrum interference or loss of spectrum coverage.

## Step 6: Course of Action Approval

- The spectrum manager consolidates units' submission of frequency proposals and provides the units with frequency assignments.
- The spectrum manager modifies the spectrum management portion of COAs according to the commander's guidance

## Step 7: Orders Production Dissemination, and Transition

- The spectrum manager produces the CEOI and disseminate to units.
- The spectrum manager provides input to Annex H (Signal) of the operations order (OPORD) that addresses all signal concerns, to include spectrum use information.

## II. SMO Support to the Warfighting Functions

Ref: ATP 6-02.70, *Techniques for Spectrum Management Operations* (Oct '19), chap. 3.

SMO enables and supports the Army's warfighting functions described in ADP 3-0, Unified Land Operations. A warfighting function is a group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives. The Army's warfighting functions are—movement and maneuver, intelligence, fires, sustainment, command and control, and protection. This chapter links Army SMO to the warfighting functions, also describes how SMO supports and enables the commander's efforts as they exercise command and control.

### Movement and Maneuver

SMO enables movement and maneuver by maintaining freedom of action within the electromagnetic spectrum. Commanders can leverage information derived from SMO to provide lethal and non-lethal effects against enemy combat capabilities while ensuring protection from adversary's use of the spectrum. SMO supports movement and maneuver by—

- Spectrum resource planning, analysis, and simulation to determine spectrum supportability over a projected movement of forces.
- Analysis, location, and direction finding of unknown and unplanned signals.
- Planning and simulating spectrum within the AO.
- Frequency deconfliction planning during movement of forces.

### Intelligence

SMO supports intelligence through the provision of spectrum situational understanding and the ability to gain a greater understanding of the EMOE. Understanding the EMOE results in successful frequency deconfliction of SDD, greater fidelity in threat recognition, and provision in support to the denial and destruction of enemies' counter-intelligence, counter-surveillance, and counter-reconnaissance systems. SMO supports intelligence by—

- Spectrum situational awareness using measurement, analysis, and assessment of signals in the AO.
- Providing a detailed caption of the EMOE for situational awareness.
- Production and promulgation of JRFL identifying protected frequencies used by friendly forces that are of critical importance, to include intelligence operations, including guarded frequencies on the JRFL to exploit an adversary's intelligence.
- Centralized databases facilitate collection management through subordinate and adjacent units.
- Deconflicting frequencies that create EMI with unmanned aircraft systems that may be conducting intelligence operations in the AO.

### Fires

SMO provides crucial support to the fires warfighting function through spectrum awareness and direct support to EW. Electromagnetic environmental effects influence the operational capability of military forces, equipment, systems, and platforms. Spectrum management operations support the fires warfighting function through mitigation of EMI amongst fires systems. SMO supports fires by—

- Coordination throughout the EMOE to prevent EMI to and from firing devices, sensors, and data links that use the spectrum.
- Coordination with the CEMA element that allows effective use of spectrum resources for EW operations.
- Integration and synchronization of CEMA by assignment and allocation of spectrum use in joint environments.

## Sustainment

The sustainment warfighting function is the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance. SMO ensures that all SDDs used for sustainment have necessary frequencies and minimal EMI.

Through coordination with EW, SMO contributes to overall sustainment in a hostile EMOE. SMO supports sustainment by—

- Providing the necessary frequencies for logistics SDDs within the EMOE conducting sustainment operations.
- Obtaining frequency clearance for logistics SDDs to conduct sustainment operations for the duration of the mission.
- Frequency deconfliction and emissions control procedures in support of sustainment operations.

## Command and Control

The command and control (C2) warfighting function develops and integrates those activities, enabling a commander to balance the art of command and the science of control. C2 emphasizes the centrality of the commander. Commanders exercise C2 by driving the operations process, knowledge management and information management, synchronization of information-related capabilities, and conducting CEMA. SMO enables C2 through the mitigation of EMI resulting from both frequency fratricide and enemy attack actions. In a contested, congested, and competitive EMOE, the C2 function must remain effective. SMO plays a vital part in the planning and management process that results in situational awareness of the EMOE.

SMO supports C2 by—

- Planning and preparing the spectrum in response to a mission.
- Assessment of the EMOE in response to the commander's intent.
- Preparation and maintenance of the EMOE database.
- Understanding the impact of a mission on friendly, neutral, adversary, enemy, joint, interagency, intergovernmental, and multinational entities.
- Collecting spectrum information and visualizing this information in quick and easy to understand formats for completion of the COP.
- Control of the spectrum through force tracking and visualization, frequency deconfliction, reprogramming, registration of SDDs.
- Development of SMO planning and management tools that support the network-centric environment (NCE) and become interoperable with Army and joint task force spectrum users.

## Protection

The protection warfighting function is the related tasks and systems that preserve the force so the commander can apply maximum combat power. SMO supports the protection warfighting function through the conduct of frequency deconfliction, interference mitigation, and support to EW defensive actions. SMO supports protection by—

- Network and frequency fratricide avoidance, detection, and mitigation.
- Developing of the JRFL to prevent frequency fratricide and mission degradation.
- Coordinating with CEMA Element to protect against blue force EMI during EW operations, such as counter radio-controlled improvised explosive device EW use.
- The spectrum manager also protects the force by recognizing the potential of electromagnetic environmental effects.

## II. The Common Operational Picture (COP)

*Ref: ATP 6-02.70, Techniques for Spectrum Management Operations (Oct '19), pp. 2-14.*

The COP is a single display of relevant information within a commander's AO tailored to user requirements and based on shared data and information shared by more than one command. The spectrum manager assists with the information collection efforts by providing detailed data of the EMOE for the commander's COP.

SMO planning tools, used in conjunction with Intelligence and EW information, allow the spectrum manager to collect spectrum-related details tailored to the commander's AO. These tools provide a visual depiction of force structure and geographical locations in a three-dimensional picture that personnel can understand quickly and easily. The following are some examples of SMO supports to the COP—

### Live Spectrum Analysis

The spectrum manager uses SMO planning tools to analyze spectrum emissions within the commander's AO. Use of information attained from the spectrum analysis is to perform EMI mitigation. SMO planning tools include—spectrum analyzers or monitoring receivers, direction-finding antennas, and analysis software. SMO planning tools can be used to show or model persistent unplanned signals that interfere with assigned frequencies during detection of EMI. SMO planning tools provide a three-dimensional picture of the EME to the commander and includes a graphical depiction of the spectrum footprint, along with recommendations for frequency reassignment to maintain communications in the AO. Using information provided by SMO planning tools and mission priorities, the commander may deem it necessary to obtain new frequencies for mission accomplishment.

### Movement of Forces to a New Location

When the commander orders movement of forces to a new area, the spectrum manager creates the proposed movement route with the SMO planning tools. The spectrum manager collaborates with adjacent units to minimize EMI with friendly forces' communications systems, sensors, and receivers throughout the movement. The SMO planning tools perform a simulation and provide COAs to determine if communication systems remain operational during movement. The SMO planning tools determine if a specific movement route with active EW systems can cause interference of friendly communications along that route. The SMO planning tools produce a report with actionable information such as sources, victims, levels, and duration of interference. This information provides the commander with supplementary information to make knowledgeable decisions.

# III. Planning Joint EMS Operations (JEMSO)

*Ref: JP 3-85, Joint Electromagnetic Spectrum Management Operations (May '20); chap. III.*

JFCs centralize JEMSO planning under the designated EMSCA and decentralize execution to ensure JEMSO unity of effort while maintaining tactical flexibility. Operations in the EMS cross all joint functions, span the OE, and are often complex and interwoven. This requires detailed prioritization, integration, and synchronization to attain EMS superiority, achieve the commander's objectives, mitigate EMI, and avoid friendly fire EA incidents (involving personnel or equipment). JEMSO planning provides the basis for the prioritization, integration, and synchronization of joint force EMS operations between the staff functions (primarily J-2, J-3, and J-6), components, and multinational partners across all phases of military operations. The CCMD JEMSOC is the lead staff element for JEMSO planning. JEMSO planning uses the joint planning process (JPP) to frame the problem; examine mission objectives; develop, analyze, and compare alternative courses of action (COAs); select the best COA; and produce the JEMSO plan or order. The JPP normally results in the development of CONOPS, OPLANs, and OPORDs. The JEMSOC ensures JEMSO are integrated throughout the command's planning process.

## Planning Process

The commander's guidance and estimate form the basis for determining components' objectives. During mission analysis, JEMSO planners develop a JEMSO staff estimate, which forms the basis for an EMS superiority approach. The staff estimate is used during COA development and analysis to determine the EMS activities and capabilities required to accomplish the mission, the JEMSO capabilities required to support operations, and the risk to the operation if EMS superiority is not achieved. When a COA is chosen, it becomes the basis for developing the JEMSO appendix, which outlines JEMSO missions, priorities, policies, processes, and procedures across all phases of the operation. The joint force components will develop component EMSO plans and submit them to the JEMSOC for integration into the JEMSO appendix under annex C (Operations). The JEMSO planning process is a formal, top-down, centralized process that integrates EMSO into the JFC's plan.

*Figure III-1 (following page) shows the types of tasks and products the JEMSOC should develop during each JPP step.*

## I. Electromagnetic Order of Battle (EOB)

The EOB is a key product the JEMSOC updates to support planning. The EOB details the strength, command structure, disposition, and operating parameters of friendly force, threat, and neutral EMS-dependent systems identified in the order of battle. This includes the identification of transmitters and receivers in an AOI, a link to systems and platforms supported, determination of their geographic location or range of mobility, characterization of their signals, EMS parameters, and, where possible, a determination of their role in the broader organizational order of battle. While the J-2 provides the information required to build the threat and neutral EOBs, the J-3, J-6, components, and supporting units provide the information necessary to build the friendly force EOB. The J-2 will also contribute to the friendly force EOB by providing information regarding ISR within the EMOE.

## II. Electromagnetic Operational Environment (EMOE) Estimate

The JEMSOC defines and characterizes the EMOE within the AOI associated with a given OA. The EMOE estimate includes sections that describe the background EME; identify factors that affect signal propagation (e.g., environmental characteristics and terrain); create a database of the known spectrum-use information; review historic EMI events within the area; and integrate the friendly, neutral, and threat EOBs.

### Define and Characterize the Electromagnetic Operational Environment (EMOE)

The situation analysis portion of the JEMSO staff estimate is where the EMOE is initially defined and characterized, forming the foundation for the JEMSO aspects of COA development, analysis, and selection.

Characterizing the EMOE is an iterative process that employs many of the tasks and methodologies associated with JIPOE. An EMOE tends to be dynamic, requiring the associated databases and analyses be updated periodically, often on a very short timeline. The physics of the EMS dictate that the military usefulness and properties of a given set of frequencies may vary periodically, based on environmental factors outside of JFC control. JEMSO planners not only must anticipate changes in both neutral and threat operations in the EMS but also need to consider potential naturally occurring EMOE changes as well. Sources and areas subject to EMI (e.g., local civilian infrastructure such as airports) should be identified as part of the EMOE.

EMOE information should be current, accurate, and accessible to authorized users. JEMSO planners should designate primary EMOE data sources to facilitate this. This source designation should be accompanied by information on the organization(s) responsible for maintaining the data sources, the associated processes and timelines for source population, requirements for access (user clearances and timelines), and the processes for dealing with data source conflicts.

Meteorological, oceanographic, and space conditions should be considered. JEMSO planners should include the effects of atmospheric and space weather on both the EMOE and all EMS-dependent systems. The various types of atmospheric conditions and phenomena can positively or negatively affect these systems. For example, atmospheric temperature inversions can increase the propagation of radio signals with frequencies in excess of 30 megahertz; high humidity and rainy climates are detrimental to IR systems; and ionospheric scintillation can adversely affect GPS, high frequency, and ultrahigh frequency transmissions. Some atmospheric effects are well known and are categorized by season and location. Planners should consult with the CCMD meteorological, oceanographic, and space staffs to determine the type of support available for their operation.

The JEMSOC will use this information to create EMOE estimates that support each step of the JPP. These EMOE estimates describe the predicted state of the EMOE at a future time and location. Components of an EMOE estimate include:

- (a) Expected state of the physical environment (e.g., METOC predictions).
- (b) Threat, neutral, and friendly force EMS-dependent systems expected to be active during that time.
- (c) Level of readiness and predicted role of the EMS-dependent systems in support of operations.
- (d) Most likely locations and range of operation of the EMS-dependent systems.
- (e) Predicted set of EMS parameters to be used.

# JEMSMO Cell Actions and Outputs as Part of Joint Planning

Ref: JP 3-85, Joint Electromagnetic Spectrum Management Operations (May '20), fig. III-1.

Planning Process Steps	Joint Electromagnetic Spectrum Operations Cell (JEMSOC) Planning Actions	JEMSOC Planning Outputs
Planning Initiation	<ul style="list-style-type: none"> <li>Review appropriate documents such as warning order and strategic assessment.</li> <li>Review joint intelligence preparation of the operational environment, desired end state, strategic effects and objectives</li> <li>Obtain order of battle and begin building electromagnetic order of battle (EOB)</li> <li>Review rules of engagement (ROE), guidance, and operational estimates</li> <li>Review operational factors within theater to identify risk to mission</li> <li>Identify organizational construct for the JEMSOC</li> <li>Identify US/multinational electromagnetic spectrum (EMS) considerations</li> <li>Identify EMS-use restrictions</li> <li>Disseminate electromagnetic interference reporting procedures</li> <li>Disseminate joint restricted frequency list requirements</li> <li>Disseminate EMS management tools and procedures</li> </ul>	<ul style="list-style-type: none"> <li>Initial EOB</li> <li>Requests for information (RFIs) on threats</li> <li>Friendly force information requirements (FFIRs)</li> <li>Data call message</li> <li>EMS management concept</li> <li>Multinational frequency assignment agreement(s) initiated</li> <li>Initiate host nation (HN) frequency coordination</li> </ul>
Mission Analysis	<ul style="list-style-type: none"> <li>Support development of intelligence estimate</li> <li>Describe how threat uses the electromagnetic operational environment (EMOE) to support operations</li> <li>Describe threat capability to deny friendly force EMS use</li> <li>Identify specified, implied, and essential electromagnetic spectrum operations (EMSO) tasks</li> <li>Identify assumptions, constraints, and restraints relevant to EMSO</li> <li>Identify planning support requirements, issue support requests</li> <li>Review available EMSO assets, identify employment authorities</li> <li>Define the EMOE area of interest</li> <li>Describe EMOE physical and environmental characteristics</li> <li>Provide EMSO perspective in support of mission requirements</li> <li>Identify EMSO opportunities for EMSO and risk to mission</li> <li>Support center of gravity (COG) decomposition and analysis</li> <li>Determine EMSO role in defeating COG</li> </ul>	<ul style="list-style-type: none"> <li>Updated EOB</li> <li>Draft initial EMS staff estimate</li> <li>List of EMSO tasks</li> <li>Assumptions, limits, constraints, and restraints</li> <li>EMSO planning guidance</li> <li>JEMSOC augmentation request</li> <li>List of EMSO capabilities potentially required</li> </ul>
Course of Action (COA) Development	<ul style="list-style-type: none"> <li>Build EOB and EMOE estimate for each COA</li> <li>Review intelligence estimate of threat and friendly force COAs</li> <li>Identify electromagnetic warfare (EW) requirements and opportunities for each COA</li> <li>Determine how EMOE must be shaped to support the COA</li> <li>Identify EMSO capabilities required to meet EW tasks</li> <li>Revise EMSO portion of COA to develop staff estimate</li> <li>Analyze COA from EMSO perspective, build mitigation methods</li> </ul>	<ul style="list-style-type: none"> <li>List of objectives, tasks, capabilities</li> <li>EOB and EMOE for each COA</li> <li>Threat and friendly force targets vulnerable to electromagnetic attack (EA)</li> <li>Initial joint task force (JTF) EMS requirements summary developed</li> </ul>
COA Analysis and Wargaming	<ul style="list-style-type: none"> <li>Analyze each COA from EMSO perspective</li> <li>Identify operations in the EMS supporting all component missions</li> <li>Identify threat capabilities that impact friendly force operations</li> <li>Identify opportunities to exploit or attack threat electromagnetic operations</li> <li>Identify possible targets for EA</li> <li>Recommend EMSO critical information requirements</li> <li>Identify the activities required to shape the electromagnetic environment to support operations and the risk to COA if EMOE is not shaped accordingly</li> </ul>	<ul style="list-style-type: none"> <li>List of EMSO assets</li> <li>Assessment of COA risk from EMSO view</li> <li>List of EA vulnerable targets</li> <li>List of targets to enable friendly force EMSO</li> <li>JTF EMS requirements summary developed</li> </ul>
COA Approval	<ul style="list-style-type: none"> <li>Compare each COA based on mission and EMSO tasks</li> <li>Compare EMSO requirements from each COA</li> <li>Review EMSO assets and capabilities needed to execute COAs</li> <li>Identify risk to COA execution from EMSO perspective</li> <li>Prepare EMSO risk assessment portion of decision brief</li> <li>Obtain EMS resources and HN approval</li> </ul>	<ul style="list-style-type: none"> <li>COA EMSO strengths and weaknesses</li> <li>EMSO risk assessment for each COA</li> <li>Risk mitigation methods</li> <li>JTF allotment plan</li> </ul>
Plan or Order Development	<ul style="list-style-type: none"> <li>Update EOB and EMS staff estimate based on COA decision</li> <li>Develop EMSO guidance</li> <li>Review joint and component concept of operations and schemes of maneuver</li> <li>Develop EMSO portion of a synchronization matrix</li> <li>Submit EMSO-related information requests and ROE</li> <li>Refine EMSO tasks from the approved COA</li> <li>Identify EMSO capability shortfalls and recommend solutions</li> <li>Update EMSO portions of operations plan</li> <li>Advise commander on EMSO issues and concerns</li> </ul>	<ul style="list-style-type: none"> <li>Initial EMOE estimate</li> <li>EMS staff estimate</li> <li>Joint electromagnetic spectrum operations (JEMSO) appendix</li> <li>Request for EMS forces</li> <li>EMSO ROEs, RFIs, and FFIRs</li> <li>Initial master net list</li> <li>JEMSO plan (includes EMS plan)</li> </ul>

See also pp. 4-41 to 4-44, cyberspace integration in the joint planning process.



# Information (Planning Considerations)

Ref: JP 6-01, *Joint Electromagnetic Spectrum Management Operations* (Mar '12), pp. III-13 to III-16.

## Information Function

The information function encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of military activities to achieve the commander's objectives and attain the end state. JEMSO enable information activities by coordinating and integrating EMS-use requirements to eliminate or mitigate EMI caused by friendly or threat forces. JEMSO also provide information activities with the means of transmitting information through the EMS.

The JFC or designated staff element may establish an information cell to coordinate the inherent informational aspects of activities that support the CONOPS. Nearly all information activities depend on, use, or exploit the EMS for at least some of their functions. JEMSO prioritization, integration, and synchronization are continuous processes and a constant consideration in information planning efforts.

EA can create decisive and enhanced effects in the information environment that provide the JFC with an operational advantage by contributing to the gaining and maintaining of information superiority. Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying a threat's ability to do the same.

When EA is employed as nonlethal fires, it can often be employed with little or no associated physical destruction. EA in support of information activities is integrated at the JFC level, through the joint targeting coordination board (JTCB) or like body, to predict collateral damage and/or effects and incorporate risk mitigation techniques.

## Military Information Support Operations (MISO)

JEMSO support and enable the joint MISO communications plan by ensuring frequencies are available for broadcast services when these are controlled by the CCDR. MISO units depend on information gathered through JEMSO (e.g., ES) and intelligence (e.g., SIGINT) sensors to warn them of threats and provide feedback about reaction to MISO broadcasts and other activities. MISO uses EP and JSIR processes to eliminate or mitigate threat EA activities or inadvertent EMI from disrupting their efforts. MISO and JEMSO coordination, especially with regards to EA, depends on timely updates to EMS operating instructions.

## Operations Security (OPSEC)

JEMSO support OPSEC by degrading threat intelligence collection against friendly units and activities. ES supports OPSEC by providing information about threat capabilities and intent to collect intelligence on friendly forces through the EMS. ES can also be used to evaluate the effectiveness of friendly force EMCON measures and recommend modifications or improvements. An effective and disciplined EMCON plan and other appropriate EP measures are important aspects of good OPSEC. OPSEC supports EMSO by concealing units and systems to deny information on the extent of EMSO capabilities. During operations, OPSEC and JEMSO staff personnel should frequently review the CCIRs in light of the dynamics of the operation. Adjustments should be recommended to the EMCON posture and other EP measures as necessary to maintain effective OPSEC.

## Military Deception (MILDEC)

JEMSO support MILDEC by using EA as deception measures; degrading threat capabilities to see, report, and process competing observables; providing threats with information received by EM means that is prone to misinterpretation; and using EP and EMCON to control EM activity observable by a threat. MILDEC frequently relies on the EMS to convey the deception to threat intelligence or tactical sensors. JEMSO planners should ensure EMS frequencies necessary to support deception plans are accounted for in EMS management databases and in the EMS operating instructions without disclosing that specific frequencies are related to deception.

Designated JEMSO planners work through the J-3 staff to coordinate and integrate JEMSO support to MILDEC operations.

## Suppression of Enemy Air Defenses (SEAD)

SEAD is a specific type of mission intended to neutralize, destroy, or temporarily degrade surface-based enemy air defenses with destructive and/or disruptive means. Joint SEAD is a broad term that includes all SEAD activities provided by one component of the joint force in support of another. SEAD missions are of critical importance to the success of any joint operation when control of the air is contested. SEAD relies on a variety of EW platforms to conduct ES and EA in its support, and JEMSO planners should coordinate closely with joint and component air planners to ensure support to SEAD missions is integrated into the overall JEMSO plan.

## EW Reprogramming

EW reprogramming is the deliberate alteration or modification of EW or target sensing systems (TSSs), or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the EME. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and TSS equipment. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and ES systems. The reprogramming of EW and TSS equipment is the responsibility of each Service or organization through its respective EW reprogramming support programs. The swift identification and resolution of reprogramming efforts is vital in gaining EMS superiority in a rapidly evolving, congested, and contested EMOE. Service reprogramming efforts include coordination with the JEMSO to ensure those reprogramming requirements are identified, processed, deconflicted, and implemented in a timely manner by all affected friendly forces. The JEMSO includes the status of EW reprogramming efforts during planning to account for potential platform vulnerabilities.

## Cybersecurity

The DOD cybersecurity program is concerned with preventative, protective, and restorative measures for information systems and the information contained therein. Many of these measures involve the use of the EMS. EP equipment, attributes, and processes assist in assuring the availability and integrity of modulated data traversing the EMOE. EA TTP assist in compromising those same qualities which threat cybersecurity seeks to protect. EMS management procedures, particularly EMI resolution, assist the application of cybersecurity policy in overcoming the problem of EM friendly fire incidents.



Refer to INFO1: *The Information Operations & Capabilities SMARTbook (Guide to Information Operations & the IRCs)*. INFO1 chapters and topics include information operations (IO defined and described), information in joint operations (joint IO), information-related capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution (IO working group, IO weighted efforts and enabling activities, intel support), fires & targeting, and information assessment.

### III. JEMSO Staff Estimate

The purpose of the JEMSO staff estimate is to inform the commander, staff, and subordinate commands how EMSO support mission accomplishment. The commander and staff use this information to support COA development and selection. JEMSO planners use the staff estimate (a primary product of mission analysis) to prepare evaluation request messages to solicit COA input from subordinate components and units to subsequently develop preliminary COAs. The JFC's JEMSOC uses the CCMD's mission, commander's estimate, objectives, intent, and CONOPS to develop COAs. During COA development and selection, JEMSO planners fully develop their estimate, providing an EMS analysis of the COAs, as well as recommendations on which COAs can be adequately supported by JEMSO. Planners should identify critical shortfalls or obstacles that impact mission accomplishment. The JEMSO staff estimate is continually updated, based on changes in the situation.

*For information on JEMSO staff estimates, refer to JP 6-01, appendix G, "Joint Electromagnetic Spectrum Operations Staff Estimate Template."*

#### EMS Superiority Approach

The EMS superiority approach ensures joint forces achieve the advantage in the EMS that permits the conduct of operations at a given time and place without prohibitive interference, while affecting an enemy's ability to do the same. The approach is comprised of the mission analysis and mission statement portions of the JEMSO staff estimate and should be documented in the EMSO section of the CONPLAN OPLAN/OPORD. This approach outlines the key missions and tasks the joint force components will carry out to achieve EMS superiority and establishes the basic relationships between the exploit, attack, protect, and manage activities the joint force will accomplish. The approach identifies key EMS users throughout the OE. It provides the framework for detailed JEMSO planning.

#### Determine Friendly EMS-Use Requirements

A joint force employs EMS-dependent systems across all functions and activities. The JEMSOC establishes the process to solicit, compile, and process joint EMS-use requirements. Components identify the EMS-dependent systems they will employ in the OE, describe the capabilities and associated EMS-use requirements, and request EMS support. The resultant data is used to build the friendly force EOB, develop the EMS superiority approach, define and characterize the EMOE, determine the supportability of each COA, build the joint EMSO plan (i.e., identifies all component and supporting unit military activities in the EMS), and provide EMSO input to OPLAN or OPORD (i.e., authorizes component military EMS activities).

### IV. JEMSO Appendix to Annex C

Once a COA is chosen, the JEMSOC develops the JEMSO appendix within annex C (Operations) for the JFC's approval. This appendix establishes procedures for C2 of forces conducting JEMSO in the JOA and includes EMS coordination measures, specifying procedures, and ROE for joint force EMS use. To provide effective operational procedures, the JEMSO appendix is integrated across all portions of the JFC's COPLANS, OPLANS, and orders. The appendix considers procedures and interfaces with the international or national frequency control authorities/systems necessary to effectively support JEMSO, augmenting forces, and JFC objectives.

*For more information, refer to JP 6-01, appendix A, "Electromagnetic Spectrum Management." Consequently, the JEMSO appendix should be planned in advance to the highest degree possible and maintained in a basic, understandable format.*

# I. Acronyms & Abbreviations

Ref: JP 3-12, *Cyberspace Operations* (Jun '18) and FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Aug '21).

## A

AOR area of responsibility  
ARCYBER U.S. Army Cyber Command

## B

BDA battle damage assessment

## C

C2 command and control  
CCDR combatant commander  
CCMD combatant command  
CCMF Cyber Combat Mission Force  
CEMA cyberspace electromagnetic activities  
CERF cyber effects request format  
CEWO cyber electromagnetic warfare officer  
CI counterintelligence  
CI/KR critical infrastructure and key resources  
CIO chief information officer  
CMF Cyber Mission Force  
CMT combat mission team  
CNMF Cyber National Mission Force  
CNMF cyber national mission force  
CNMF-HQ Cyber National Mission Force Headquarters  
CO cyberspace operations  
COA course of action  
COCOM combatant command (command authority)  
CO-IPE cyberspace operations-integrated planning element  
CONOPS concept of operations  
CONPLAN concept plan  
COP common operational picture  
CPF Cyber Protection Force  
CPT cyberspace protection team  
CSA combat support agency  
CSSP cybersecurity service provider  
CST combat support team

## D

D3A decide, detect, deliver, and assess  
DACO directive authority for cyberspace operations  
DC3 Department of Defense Cyber Crime Center  
DCI defense critical infrastructure  
DCO defensive cyberspace operations  
DCO-IDM defensive cyberspace operations-internal defensive measures  
DCO-RA defensive cyberspace operations-response actions  
DCO-RA defensive cyberspace operations-response actions  
DHS Department of Homeland Security  
DIA Defense Intelligence Agency  
DIB defense industrial base  
DISA Defense Information Systems Agency  
DOD Department of Defense  
DODIN Department of Defense information network  
DODIN-A Department of Defense information network-Army  
DSCA defense support of civil authorities

## E

EA electromagnetic attack  
EMI electromagnetic interference  
EMOE electromagnetic operational environment  
EMS electromagnetic spectrum  
EMSO electromagnetic spectrum operations  
EP electromagnetic protection  
ES electromagnetic support  
EW electromagnetic warfare  
EXORD execute order

---

<b>G</b>	
GCC	geographic combatant commander
GFMIG	Global Force Management Implementation Guidance

---

<b>I</b>	
I2CEWS	intelligence, information, cyber, electromagnetic warfare and space
IAW	in accordance with
IC	intelligence community
IGL	intelligence gain/loss
IJSTO	integrated joint special technical operations
IO	information operations
IP	Internet protocol
IPB	intelligence preparation of the battlefield
IR	intelligence requirement
IRC	information-related capability
ISP	Internet service provider
ISR	intelligence, surveillance, and reconnaissance
IT	information technology

---

<b>J</b>	
JEMSO	joint electromagnetic spectrum operations
JEMSOC	joint electromagnetic spectrum operations cell
JFC	joint force commander
JFHQ-C	Joint Force Headquarters-Cyber
JFHQ-C	joint force headquarters-cyberspace
JIACG	joint interagency coordination group
JOA	joint operations area
JP	joint publication
JPP	joint planning process
JS	Joint Staff
JTF	joint task force
JTL	joint target list

---

<b>L</b>	
LE	law enforcement
LOC	line of communications

---

<b>M</b>	
MILDEC	military deception
MISO	military information support operations
MNF	multinational force
MOE	measure of effectiveness

---

MOP	measure of performance
MTFP	mission-tailored force package
NCO	noncommissioned officer
NETCOM	United States Army Network Enterprise Technology Command

---

<b>N</b>	
NIPRNET	Non-classified Internet Protocol Router Network
NMT	national mission team
NST	national support team

---

<b>O</b>	
OA	operational area
OCO	offensive cyberspace operations
OE	operational environment
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSC	offensive space control
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence

---

<b>P</b>	
PIT	platform information technology
PN	partner nation
PPD	Presidential policy directive

---

<b>R</b>	
RFI	request for information
RFS	request for support
ROE	rules of engagement

---

<b>S</b>	
SATCOM	satellite communications
SCC	Service cyberspace component
SecDef	Secretary of Defense
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network

---

<b>T</b>	
TACON	tactical control
TCPED	tasking, collection, processing, exploitation, and dissemination
TSS	targeting sensing software
TST	time-sensitive target

---

<b>U</b>	
USC	United States Code
USCYBERCOM	U.S. Cyber Command

---

## \* 8-2 I. Abbreviations & Acronyms

# (CYBER1-1)

## II. Glossary

*Ref: JP 3-12, Cyberspace Operations (Jun '18) and FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21). This combined glossary lists acronyms and terms with Army, multi-Service, or joint definitions, and other selected terms. The proponent publication for a term is listed in parentheses after the definition.*

### A

**Adversary.** A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

**Army design methodology.** A methodology for applying critical and creative thinking to understand, visualize, and describe problems and approaches to solving them. Also called ADM. (ADP 5-0)

**Assessment.** 1) A continuous process that measures the overall effectiveness of employing capabilities during military operations. 2) Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. 3) Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4) Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 3-0)

### C

**Chaff.** Radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion purposes. (JP 3-85)

**combat power.** The total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time. (ADP 3-0)

**constraint.** A restriction placed on the command by a higher command. (FM 6-0)

**countermeasures.** That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 3-85)

**cyberspace attack.** Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires. (JP 3-12)

**cyberspace capability.** A device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. (Approved for inclusion in the DOD Dictionary.)

**cyberspace defense.** Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include 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. (Approved for inclusion in the DOD Dictionary.)

**cyberspace defense.** Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include 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. (JP 3-12)

**cyberspace electromagnetic activities.** The process of planning, integrating, and synchronizing cyberspace operations and electromagnetic warfare operations in support of unified land operations. Also called CEMA. (ADP 3-0)

**cyberspace exploitation.** Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations. (JP 3-12)

**cyberspace operation.** The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Also see CO. (JP 3-0)

**cyberspace security.** Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (JP 3-12)

**cyberspace superiority.** The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference. (Approved for incorporation into the DOD Dictionary.)

**cyberspace.** A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

---

## D

**defeat.** To render a force incapable of achieving its objectives. (ADP 3-0)

**defensive cyberspace operations.** Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. Also called DCO. (JP 3-12)

**defensive cyberspace operations-internal defensive measures.** Operations in which authorized defense actions occur within the defended portion of cyberspace. Also called DCO-IDM. (JP 3-12)

**defensive cyberspace operations-response actions.** Operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without permission of the owner of the affected system. Also called DCO-RA. (JP 3-12)

**Department of Defense information network.** The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. Also called DODIN. (JP 6-0)

**Department of Defense information network operations.** Operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network. Also called DODIN operations. (JP 3-12)

**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)

**directed energy.** An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called DE. (JP 3-85)

**directed-energy warfare.** Military actions involving the use of directed-energy weapons, devices, and countermeasures. Also called DEW. (JP 3-85)

## \* 8-4 II. Glossary



**directed-energy weapon.** A weapon or system that uses directed energy to incapacitate, damage, or destroy enemy equipment, facilities, and/or personnel. (JP 3-85)

**direction finding.** A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. Also called DF. (JP 3-85)

**directive authority for cyberspace operations.** The authority to issue orders and directives to all Department of Defense components to execute global Department of Defense information network operations and defensive cyberspace operations internal defensive measures. Also called DACO. (Approved for inclusion in the DOD Dictionary.)

**dynamic targeting.** Targeting that prosecutes targets identified too late or not selected for action in time to be included in deliberate targeting. (JP 3-60)

---

## E

**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. Also called EA. (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. Also called EMC. (JP 3-85)

**electromagnetic hardening.** Actions 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 intrusion.** The intentional insertion of electromagnetic energy into transmission paths in any manner. The objective of electromagnetic intrusion is to deceive threat operators or cause 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, and 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.** The intentional radiation designed to be introduced into the devices or systems of adversaries to learn 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. Also called EP. (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 security.** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations (e.g., radar). (JP 3-85)

**electromagnetic spectrum superiority.** That degree of control in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting the threat's ability to do the same. (JP 3-85)

**electromagnetic support.** Division of electromagnetic warfare involving actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conduct of future operations. Also called ES. (JP 3-85)

**electromagnetic vulnerability.** The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of electromagnetic environmental effects. (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)

**enemy.** An enemy is a party identified as hostile against which the use of force is authorized. (ADP 3-0)

**essential task.** A specified or implied task that must be executed to accomplish the mission. (FM 6-0)

**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)

---

## H

**hazard.** A condition with the potential to cause injury, illness, or death of personnel, damage to or loss of equipment or property, or mission degradation. (JP 3-33)

**high-payoff target.** A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. Also called HPT. (JP 3-60)

**high-value target.** A target the enemy commander requires for the successful completion of the mission. (JP 3-60)

**hybrid threat.** A hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements acting in concert to achieve mutually benefitting effects. (ADP 3-0)

---

## I

**implied task.** A task that must be performed to accomplish a specified task or mission but is not stated in the higher headquarters' order. (FM 6-0)

**information assurance.** None. (Approved for removal from the DOD Dictionary.)

**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)

**information operations.** The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO. (JP 3-13)

**intelligence operations.** The tasks undertaken by military intelligence units through the intelligences disciplines to obtain information to satisfy validated requirements. (ADP 2-0)

**intelligence preparation of the battlefield.** 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. Also called IPB. (ATP 2-01.3)

**intelligence.** 1) The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2) The activities that result in the product. 3) The organizations engaged in such activities. (JP 2-0)

---

## K

**knowledge management.** The process of enabling knowledge flow to enhance shared understanding, learning, and decision making. (ADP 6-0)

---

## N

**named area of interest.** The geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected. Also called NAI. (JP 2-01.3)

---

## O

**offensive cyberspace operations.** Missions intended to project power in and through cyberspace. Also called OCO. (JP 3-12)

**operational environment.** A composite of the conditions, circumstances, and influences that affect the employment of capabilities and impact the decisions of the commander assigned responsibility for it. Also called OE. (JP 3-0)

**operational initiative.** The setting or tempo and terms of action throughout an operation. (ADP 3-0)

**operations process.** The major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation. (ADP 5-0)

**operations security.** A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. Also called OPSEC. (JP 3-13.3)

---

## P

**planning.** The art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. (ADP 5-0)

**position of relative advantage.** 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. (ADP 3.0)

**preparation.** Those activities performed by units and Soldiers to improve their ability to execute an operation. (ADP 5.0)

**priority of fires.** The commander's guidance to the staff, subordinate commanders, fires planners, and supporting agencies to employ fires in accordance with the relative importance of a unit's mission. (FM 3-09)

**priority of support.** A priority set by the commander to ensure a subordinate unit has support in accordance with its relative importance to accomplish the mission. (ADP 5-0)

---

---

## R

**radio frequency countermeasures.** Any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision-guided and sensor systems. (JP 3-85)

**risk management.** The process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

---

## S

**scheme of fires.** The detailed, logical sequence of targets and fire support events to find and engage targets to support commander's objectives. (JP 3-09)

**specified task.** A task specifically assigned to an organization by its higher headquarters. (FM 6-0)

---

## T

**target.** An entity or object that performs a function for the adversary considered for possible engagement or other actions. See also objective area. (JP 3-60)

**target area of interest.** The geographical area where high-valued targets can be acquired and engaged by friendly forces. (JP 2-01.3)

**targeting.** The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

---

## W

**warfighting function.** A group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives. (ADP 3-0)

**wartime reserve modes.** Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasure systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. (JP 3-85)



# (CYBER1-1) Index

1st Information Operations Command, 6-10

## A

Accidents and Natural Hazards, 1-13  
Acronyms, 8-1  
Airborne Electronic Attack, 3-26  
Airborne Electromagnetic Attack Support, 4-28  
ANNEX C—OPERATIONS, 4-35  
ANNEX H—SIGNAL, 4-35  
Anonymity, 1-13  
Anticipated Operational Environments, 0-7  
Appendix 12 to Annex C, 4-35  
Army Cyber Operations and Integration Center (ACOIC), 6-12  
Army Design Methodology, 4-2  
Army Enterprise Service Desk, 6-12  
Army Information Warfare Operations Center, 2-27  
Army Organizations, 2-27  
Assess, 4-33  
Assessment, 1-55, 2-39  
Assignment of Cyberspace Forces, 1-23  
Assistant Chief of Staff, Intelligence, 2-32  
Assistant Chief of Staff, Signal, 2-33  
Authorities, 1-30

## B

Battalion Electronic Warfare Personnel, 3-13

## C

CDRUSCYBERCOM, 1-33  
CI/KR Protection, 1-30

Civil Considerations Data Files, Overlays, and Assessments, 4-h

Civil-Military Operations (CMO), 0-14, 4-48  
Close Air Support (CAS), 3-24  
Command and Control (C2), 1-48, 2-27  
Commander's Communication Synchronization (CCS), 4-46  
Commander's Role, 2-28  
Common Operational Picture (COP), 5-14  
Company CREW Specialists, 3-16  
Competition Continuum, 2-16  
Concealment, 3-32  
Conflict and Competition, 2-16  
Congested Environments, 2-10  
Connectivity and Access, 1-7  
Considerations When Targeting, 4-34  
Contemporary Operational Environment, 0-6  
Contested Environments, 2-10  
Continuity of Operations, 7-30  
Core Activities 1-15  
Core Competencies, 2-12  
Counter Radio-Controlled Improvised Device (CREW), 3-28  
Critical Capabilities, 6-38  
Critical Variables, 0-6  
Cyber Attack, 7-26  
Cyber Attack Tools, 7-18  
Cyber Combat Mission Force (CCMF), 1-10  
Cyber Effects Request Format (CERF), 4-9, 4-11

Cyber Electromagnetic Warfare Officer (CEWO), 2-30, 3-12

Cyber Kill Chain, 4-1  
Cyber Mission Force (CMF), 1-10  
Cyber National Mission Force (CNMF), 1-1  
Cyber Protection Force (CPF), 1-10  
Cyber Threat, 0-2  
Cyber Warfare Officer or Cyber-Operations Officer, 2-31  
Cyber-Persona Layer, 2-6  
Cyber-Personal Layer, 1-3, 1-3  
Cybersecurity, 7-1  
Cybersecurity Functions, 7-13, 7-15  
Cybersecurity Fundamentals, 7-1  
Cybersecurity Performance, 7-12  
Cybersecurity Principles, 7-3  
Cybersecurity Risk Management, 7-2  
Cyberspace, 0-1  
Cyberspace Actions, 1-20, 2-21  
Cyberspace and the Electromagnetic Spectrum, 2-1, 2-2  
Cyberspace Attack, 1-21, 2-22  
Cyberspace Defense, 1-21, 2-21, 7-10  
Cyberspace Domain, 2-6  
Cyberspace-Enabled Activities, 1-15  
Cyberspace (CEMA) in Operations Orders, 4-35  
Cyberspace (CEMA) Operations Planning, 4-1  
Cyberspace Electromagnetic Activities (CEMA) Section, 2-29

Cyberspace Electromagnetic Activities (CEMA) Working Group, 2-29

Cyberspace Electromagnetic Activities at Corps and Below, 2-28

Cyberspace Electromagnetic Activities Spectrum Manager, 2-31

Cyberspace Exploitation, 1-21, 2-21

Cyberspace Layer Model, 1-2

Cyberspace Missions, 0-1, 1-15, 2-19

Cyberspace Operations (CO), 0-1, 0-15, 1-1, 2-17, 4-48

Cyberspace Operations & EW Logic Chart, 2-3

Cyberspace Operations (Missions & Actions), 2-19

Cyberspace Operations Forces, 1-10

Cyberspace Security, 1-20, 2-21

## D

DCO-IDM, 1-19, 2-7

DCO-RA, 1-19, 2-7

Decide, 4-32

Deconflicting the Electromagnetic Spectrum, 3-19

Deconfliction, 1-52

Defense Information Systems Agency (DISA), 6-9

Defense of Non-DOD Cyberspace, 1-19

Defensive Cyberspace Operations (DCO), 1-19, 2-18

Defensive Cyberspace Operations Internal Defensive Measures (DCO-IDM), 2-20

Defensive Cyberspace Operations Response Action (DCO-RA), 2-20

Defensive Electromagnetic Attack, 3-2, 3-28

Define the Operational Environment, 4-b

Deliver, 4-33

Deny, 1-22

Department of Defense Information Network (DODIN) Operations, 1-6, 2-6, 2-18, 6-1

Describe Environmental Effects on Operations, 4-e

Detect, 4-33

Detect Function, 7-23

Detection, 7-29

Determine Threat Courses of Action, 4-n

Direction Finding (DF), 3-36

DOD Information Network (DODIN), 1-6, 2-6, 2-18, 6-1

DOD Ordinary Business Operations, 1-17

DODIN Enterprise Management, 6-36

DODIN Network Operations Components, 6-35

DODIN Operations Operational Construct, 6-36

DODIN Operations, 1-18

DODIN, 1-6, 2-6, 6-1

## E

Electromagnetic Attack (EA), 3-2

Electromagnetic Attack Request, 4-27

Electromagnetic Environment (EME), 5-2

Electromagnetic Environment (EME) Survey, 3-36

Electromagnetic Environmental Effects (E3), 5-8

Electromagnetic Interference (EMI), 3-10, 3-31

Electromagnetic Interference (EMI) Battle Drill, 3-33

Electromagnetic Jamming, 3-31

Electromagnetic Operational Environment (EMOE), 5-2

Electromagnetic Order of Battle (EOB), 5-15

Electromagnetic Protection (EP), 3-6

Electromagnetic Pulse (EMP), 5-8

Electromagnetic Spectrum (EMS), 2-1, 5-2

Electromagnetic Spectrum (EMS) Factors, 1-52

Electromagnetic Spectrum Operations (EMSO), 5-1

Electromagnetic Spectrum Superiority, 2-17

Electromagnetic Support (ES), 3-8

Electromagnetic Warfare (EW), 3-1

Electromagnetic Warfare (EW) Organizations, 2-36

Electronic Attack (EA), 5-6

Electronic Attack Effects, 3-21

Electronic Attack Techniques, 3-21

Electronic Protection Techniques, 3-29

Electronic Reconnaissance, 3-35

Electronic Warfare Assessment, 4-26

Electronic Warfare Configurations, 4-23

Electronic Warfare Control Authority, 3-16

Electronic Warfare Employment Considerations, 4-24

Electronic Warfare Execution, 3-20

Electronic Warfare Personnel, 3-11

Electronic Warfare Planning, 4-15

Electronic Warfare Preparation, 3-17

Electronic Warfare Running Estimate, 4-16

Electronic Warfare Support Techniques, 3-35

Electronic Warfare Technician, 3-12

EMOE Estimate, 5-16

EMS Superiority Approach, 5-20

Enabled Effects, 6-38, 7-5

Enterprise Management Activities, 6-40

Enterprise Operations Center, 6-17

Equipment and Communications Enhancements, 3-34  
 Evaluate the Threat, 4-i  
 Event Matrix, 4-q  
 Event Template, 4-p  
 Execution, 2-39  
 Exploitation, 5-6

## F

Fires Support Element, 2-34  
 Frequency Interference Resolution, 3-10  
 Frequency Interference Resolution, 5-9  
 Friendly EMS-Use Requirements, 5-20  
 Functional Network Operations and Security Centers (NOSC), 6-13  
 Functional Services, 6-36  
 Fundamental Principles, 2-12

## G

G-6 or S-6 Spectrum Manager, 2-34  
 Geographic Combatant Commander (GCC), 6-14  
 Geography Challenges, 1-13  
 Global Cyber Threat, 0-2  
 Glossary, 8-3

## H

Hazards, 2-11  
 HERF, 5-8  
 HERO, 5-8  
 HERP, 5-8  
 High-Altitude Electromagnetic Pulse (HEMP), 5-8  
 High-Value Targets, 4-m

## I

Identify Vulnerabilities, 7-14  
 Individuals or Small Group Threat, 1-12  
 Information, 0-10, 1-28  
 Information (Planning Considerations), 5-18  
 Information Assurance (IA), 4-49  
 Information Assurance Vulnerability Management (IAVM), 7-30  
 Information Collection, 2-40

Information Environment, 0-10, 1-8  
 Information Environment Operations (IEO), 0-9, 1-9  
 Information Function, 0-10  
 Information Function Activities, 0-12  
 Information Operations (IO), 0-11, 2-25, 4-44, 4-45  
 Information Operations Officer or Representative, 2-34  
 Information Operations Planning, 4-51  
 Information Systems Security, 7-26  
 Information-Influence Relational Framework, 4-45  
 Integrating / Coordinating Functions of IO, 4-45  
 Integrating Cyberspace Operations, 1-9  
 Integrating Processes, 2-40  
 Integration of Cyberspace Fires, 1-53  
 Integration through the Operations Process, 2-37  
 Intelligence, 4-49  
 Intelligence and Operational Analytic Support, 1-43  
 Intelligence Gain/Loss (IGL), 1-44  
 Intelligence Operations, 2-23  
 Intelligence Preparation of the Battlefield (IPB), 2-40, 4-a  
 Intelligence Requirements (IRs), 1-43, 4-44  
 Intelligence, Information, Cyber, EW, & Space (I2CEWS), 2-36  
 Interorganizational Considerations, 1-57  
 Interrelationship with Other Operations, 2-23  
 ISR in Cyberspace, 1-45

## J

Jamming, 3-31  
 JEMSMO Cell Actions and Outputs, 5-17  
 JEMSO Actions, 5-6  
 JEMSO Staff Estimate, 5-20

Joint Cyberspace Center (JCC), 6-14  
 Joint Cyberspace Operations, 1-1  
 Joint Electromagnetic Spectrum Operations (JEMSO), 4-50, 5-5  
 Joint Functions, 0-10, 1-24  
 Joint Interagency Coordination Group (JIACG), 4-47  
 Joint Planning Group (JPG), 4-51  
 Joint Planning Process (JPP), 1-39, 4-41  
 Joint Restricted Frequency List (JRFL), 4-22

## K

Key Leader Engagement (KLE), 0-14, 4-50  
 Key Terrain, 1-8  
 Knowledge Management, 2-41

## L

Large Scale Combat Operations, 3-28  
 Legal Considerations, 1-38  
 Leveraging Information, 0-14  
 Live Spectrum Analysis, 5-14  
 Location and Ownership, 1-6  
 Logical Network Layer, 1-3, 2-6

## M

Manage, 5-7  
 Manipulate, 1-22  
 Measures of Effectiveness (MOEs), 1-56  
 Measures of Performance (MOPs), 1-56  
 Military Deception (MILDEC), 0-14, 4-49  
 Military Decision-Making Process (MDMP), 4-2  
 Military Information Support Operations (MISO), 0-14, 4-49  
 Mission Variables (METT-TC), 2-9  
 Mission-Tailored Force Package (MTFP), 1-49



Mitigating Insider Threats, 7-27  
 Modified Combined Obstacle Overlay, 4-g  
 Multi-Domain Extended Battlefield, 0-8, 2-4, 2-16  
 Multinational Considerations, 1-58  
 National Incident Response, 1-29  
 National Intelligence Operations, 1-17  
 Nation-State Threat, 1-12

## N

Nature of Cyberspace, 1-2  
 Non-State Threats, 1-12

## O

Offensive Cyberspace Operations (OCO), 1-18, 2-20  
 Offensive Electromagnetic Attack, 3-2  
 Open-Source Intelligence (OSINT), 1-45  
 Operational Environment (OE), 0-6, 1-7, 2-4  
 Operational Initiative, 2-4  
 Operational Resilience, 7-8  
 Operational Risks, 2-42  
 Operational Variables (PMESII-PT), 2-8  
 Operations Orders, 4-35  
 Operations Process, 2-37  
 Operations Security (OP-SEC), 0-15, 4-50  
 Operations Security Risks, 2-43

## P

Phasing, 4-54  
 Physical Network Layer, 1-3, 2-6  
 Planning, 2-38, 4-1  
 Planning Considerations, 1-39  
 Planning Insights, 4-44  
 Planning Joint EMS Operations (JEMSO), 5-15  
 Planning Timelines, 1-40  
 Policy Risks, 2-43  
 Positions of Relative Advantage, 2-16

Preparation, 2-38  
 Protect, 5-6  
 Protect Function, 7-21  
 Protection, 7-25  
 Protection Levels, 7-27  
 Public Affairs (PA), 0-14, 4-48

## R

Reaction, 7-29  
 Recover Function, 7-24  
 Remedial Electronic Protection Techniques, 3-32  
 Requesting Cyberspace Effects, 4-9  
 Respond Function, 7-24  
 Risk Concerns, 1-53  
 Risk Management, 2-41  
 Risk Management Framework, 7-6  
 Risks In Cyberspace and the EMS, 2-42  
 Roles and Responsibilities, 1-30

## S

Scanning and Remediation, 7-30  
 Sensing Activity Distinctions, 3-18  
 Services' Cyberspace Doctrine, 1-4  
 SMO inputs to the MDMP, 5-10  
 SMO Support to the Warfighting Functions, 5-12  
 Space Operations, 0-15, 4-49, 2-24  
 Special Technical Operations (STO), 0-15, 4-50  
 Spectrum Management, 3-10, 5-9  
 Spectrum Management Operations (SMO/JEMSO), 3-10, 5-4, 5-1  
 Spectrum Management Operations Core Functions, 5-5  
 Spectrum Manager, 3-13  
 Staff and Support at Corps and Below, 2-32  
 Staff Judge Advocate, 2-34

Staff Members and Electronic Warfare, 3-14  
 Strategic Communication (SC), 4-46  
 Synchronization, 1-52

## T

Target Access, 1-46  
 Target Nomination and Synchronization, 1-46  
 Targeting (D3A), 1-46, 2-41, 4-29  
 Targeting Crosswalk, 4-31  
 Targeting Methodology, 4-30  
 Technical Risks, 2-42  
 Technology Challenges, 1-13  
 Terrain Effects Matrix, 4-h  
 Theater Network Operations Control Center (TNCC), 6-14  
 Threat Activities, 7-14  
 Threat Capabilities, 4-k  
 Threat Description Table, 4-f  
 Threat Detection and Characterization, 1-44  
 Threat Electronic Attack, 3-32  
 Threat Model, 4-l  
 Threat Overlay, 4-f  
 Threat Situation Template, 4-o  
 Threats, 1-12, 2-10  
 Time-Sensitive Targets (TSTs), 1-48  
 Tools of Cyber Attacks, 7-18  
 Trends and Characteristics, 2-10

## U

U.S. Army Network Enterprise Technology Command (NETCOM), 6-10  
 United States Army Cyber Command (ARCYBER), 2-27, 6-10  
 United States Code, 1-31  
 United States Cyber Command (USCYBERCOM), 1-10, 6-9

## W

Warfighting Functions, 2-14  
 Warning Intelligence, 1-45  
 Weather, Light, and Illumination Charts or Tables, 4-h



# SMARTbooks

INTELLECTUAL FUEL FOR THE MILITARY

Recognized as a **“whole of government”** doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a **comprehensive professional library** designed with all levels of Soldiers, Sailors, Airmen, Marines and Civilians in mind.



The SMARTbook reference series is used by **military, national security, and government professionals** around the world at the organizational/ institutional level; operational units and agencies across the full range of operations and activities; military/government education and professional development courses; combatant command and joint force headquarters; and allied, coalition and multinational partner support and training.

Download FREE samples and SAVE 15% everyday at:  
**[www.TheLightningPress.com](http://www.TheLightningPress.com)**



The Lightning Press is a **service-disabled, veteran-owned small business**, DOD-approved vendor and federally registered — to include the SAM, WAWF, FBO, and FEDPAY.

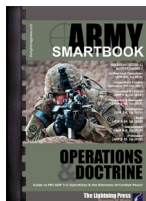


# SMARTbooks

INTELLECTUAL FUEL FOR THE MILITARY

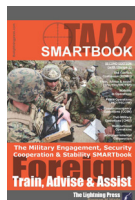
## MILITARY REFERENCE: SERVICE-SPECIFIC

Recognized as a “whole of government” doctrinal reference standard by military professionals around the world, SMARTbooks comprise a comprehensive professional library.



## MILITARY REFERENCE: MULTI-SERVICE & SPECIALTY

SMARTbooks can be used as quick reference guides during operations, as study guides at professional development courses, and as checklists in support of training.



## JOINT STRATEGIC, INTERAGENCY, & NATIONAL SECURITY

The 21st century presents a global environment characterized by regional instability, failed states, weapons proliferation, global terrorism and unconventional threats.

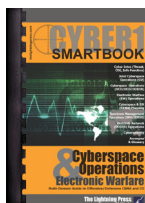


The Lightning Press is a **service-disabled, veteran-owned small business**, DOD-approved vendor and federally registered — to include the SAM, WAWF, FBO, and FEDPAY.

# RECOGNIZED AS THE DOCTRINAL REFERENCE STANDARD BY MILITARY PROFESSIONALS AROUND THE WORLD.

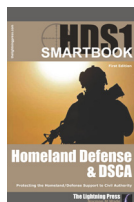
## THREAT, OPFOR, REGIONAL & CULTURAL

In today's complicated and uncertain world, the military must be ready to meet the challenges of any type of conflict, in all kinds of places, and against all kinds of threats.



## HOMELAND DEFENSE, DSCA, & DISASTER RESPONSE

Disaster can strike anytime, anywhere. It takes many forms—a hurricane, an earthquake, a tornado, a flood, a fire, a hazardous spill, or an act of terrorism.



## DIGITAL SMARTBOOKS (eBooks)

In addition to paperback, SMARTbooks are also available in digital (eBook) format. Our digital SMARTbooks are for use with Adobe Digital Editions and can be used on up to **six computers and six devices**, with free software available for **85+ devices and platforms—including PC/MAC, iPad and iPhone, Android tablets and smartphones, Nook, and more!** Digital SMARTbooks are also available for the **Kindle Fire** (using Bluefire Reader for Android).



Download FREE samples and SAVE 15% everyday at:  
**[www.TheLightningPress.com](http://www.TheLightningPress.com)**

# Purchase/Order

**SMARTsavings on SMARTbooks!** Save big when you order our titles together in a SMARTset bundle. It's the most popular & least expensive way to buy, and a great way to build your professional library. If you need a quote or have special requests, please contact us by one of the methods below!

View, download **FREE** samples and purchase online:

**www.TheLightningPress.com**



## Order **SECURE** Online

**Web:** [www.TheLightningPress.com](http://www.TheLightningPress.com)

**Email:** [SMARTbooks@TheLightningPress.com](mailto:SMARTbooks@TheLightningPress.com)



## 24-hour Order & Customer Service Line

Place your order (or leave a voicemail)  
at 1-800-997-8827



## Phone Orders, Customer Service & Quotes

Live customer service and phone orders available  
Mon - Fri 0900-1800 EST at (863) 409-8084



## Mail, Check & Money Order

2227 Arrowhead Blvd., Lakeland, FL 33813

## Government/Unit/Bulk Sales



The Lightning Press is a **service-disabled, veteran-owned small business**, DOD-approved vendor and federally registered—to include the SAM, WAWF, FBO, and FEDPAY.

We accept and process both **Government Purchase Cards** (GPC/GPC) and **Purchase Orders** (PO/PR&Cs).

**Keep your SMARTbook up-to-date with the latest doctrine!** In addition to revisions, we publish incremental "**SMARTupdates**" when feasible to update changes in doctrine or new publications. These SMARTupdates are printed/produced in a format that allow the reader to insert the change pages into the original GBC-bound book by simply opening the comb-binding and replacing affected pages. Learn more and sign-up at: [www.thelightningpress.com/smartupdates/](http://www.thelightningpress.com/smartupdates/)

