thelightningpress.com

CYBER1 SMARTBOOK

Cyberspace & Operations Electronic Warfare

Multi-Domain Guide to Offensive/Defensive CEMA and CO

The Lightning Press

Norman M Wade

thelightningpress.com

CYBER1 SMARTBOOK

& Cyberspace Operations Electronic Warfare

Multi-Domain Guide to Offensive / Defensive CEMA and CO

The Lightning Press
Norman M Wade

The Lightning Press

2227 Arrowhead Blvd.
Lakeland, FL 33813
24-hour Order/Voicemail: 1-800-997-8827
E-mail: SMARTbooks@TheLightningPress.com
www.TheLightningPress.com

(CYBER1) The Cyberspace Operations & Electronic Warfare SMARTbook

Multi-Domain Guide to Offensive/Defensive CEMA and CO

CYBER1: The Cyberspace Operations & Electronic Warfare SMARTbook (Multi-Domain Guide to Offensive/Defensive CEMA and CO) topics and chapters include cyber intro (global threat, contemporary operating environment, information as a joint function), joint cyberspace operations (CO), cyberspace operations (OCO/DCO/DODIN), electronic warfare (EW) operations, cyber & EW (CEMA) planning, spectrum management operations (SMO/JEMSO), DoD information network (DODIN) operations, acronyms/ abbreviations, and a cross-referenced glossary of cyber terms.

ISBN: 978-1-935886-71-6

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."

Credits: Cover image licensed from Shutterstock.com. All other photos courtesy Dept. of the Army and/or Dept. of Defense and credited individually where applicable.

Printed and bound in the United States of America.

(CYBER1) 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.

Electronic warfare (EW) is any 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: electronic attack, electronic protection, and electronic warfare 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**!

(CYBER1) 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.

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 5-0	Jun 2017	Joint Planning
JP 6-01	Mar 2012	Joint Electromagnetic Spectrum Management Operations

Field Manuals (FMs) and Training Circulars (TCs)

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

Army Tactics, Techniques and Procedures (ATPs/ATTPs)

ATP 3-36	Dec 2014	Electronic Warfare Techniques
ATP 6-02.70	Dec 2015	Techniques for Spectrum Management Operations
ATP 6-02.71	Apr 2019	Techniques for Department of Defense Information Network Operations

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

(CYBER1) Table of Contents

Intro

Introduction (Threat/COE/Info)

Chap 1

Joint Cyberspace Operations

Chap 2

Cyberspace (CEMA) Operations

Chap 3

Electronic Warfare Operations

Chap 4

Cyberspace & EW (CEMA) Planning

Chap 5

Spectrum Management Operations (SMO/JEMSO)

Chap 6

Dept of Defense Info Network (DODIN) Ops

Chap 7 Cybersecurity

Chap 8 Acronyms & Glossary

Intro

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, 2-1, and 2-13.*

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. Various DOD agencies and components conduct national intelligence, ordinary business, and other activities in cyberspace. Although discussed briefly here for context, these activities are guided by DOD policies concerning CO. While joint doctrine does apply to CSAs where it directly relates to their mission to support military forces, CSAs and other DOD agencies and activities also conduct various CO activities that are considered cyberspace-enabled activities. *See pp. 1-15 and 2-4.*

Cyberspace Missions

All actions in cyberspace that are not cyberspace-enabled activities are taken as part of one of three cyberspace missions: OCO, DCO, or DODIN operations. These three mission types comprehensively cover the activities of the cyberspace forces. The successful execution of CO requires integration and synchronization of these missions. Military cyberspace missions and their included actions are normally authorized by a military order (e.g., execute order [EXORD], operation order [OPORD], tasking order, verbal order), referred to hereafter as mission order, and by authority derived from DOD policy memorandum, directive, or instruction. Cyberspace missions are categorized as OCO, DCO, or DODIN operations based only on the intent or objective of the issuing authority, not based on the cyberspace actions executed, the type of military authority used, the forces assigned to the mission, or the cyberspace capabilities used. *See pp. 1-15 and 2-5.*

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.

- Russian intelligence and security services will continue targeting US information systems, as well as the networks of our NATO and Five Eyes partners, for technical information, military plans, and insight into our governments' policies.
- Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.

Iran

Iran continues to present a cyber espionage and attack threat. Iran uses increasingly sophisticated cyber techniques to conduct espionage; it is also attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries. Tehran also uses social media platforms to target US and allied audiences, an issue discussed in the Online Influence Operations and Election Interference section of this report.

- Iranian cyber actors are targeting US Government officials, government organizations, and companies to gain intelligence and position themselves for future cyber operations.
- Iran has been preparing for cyber attacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017.

North Korea

North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks. North Korea continues to use cyber capabilities to steal from financial institutions to generate revenue. Pyongyang's cybercrime operations include attempts to steal more than $1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated $81 million from the New York Federal Reserve account of Bangladesh's central bank.

Nonstate and Unattributed Actors

Foreign cyber criminals will continue to conduct for-profit, cyber-enabled theft and extortion against US networks. We anticipate that financially motivated cyber criminals very likely will expand their targets in the United States in the next few years. Their actions could increasingly disrupt US critical infrastructure in the health care, financial, government, and emergency service sectors, based on the patterns of activities against these sectors in the last few years.

Terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims. Terrorist groups could cause some disruptive effects—defacing websites or executing denial-of-service attacks against poorly protected networks—with little to no warning.

The growing availability and use of publicly and commercially available cyber tools is increasing the overall volume of unattributed cyber activity around the world. The use of these tools increases the risk of misattributions and misdirected responses by both governments and the private sector.

See pp. 7-16 to 7-17 for discussion of cyber threat activities and pp. 7-18 to 7-19 for cyber attack tools. See also p. 2-24 for discussion of threats in cyberspace from FM 3-12.

D. 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.

Refer to TRADOC PAM 525-3-1, The U.S. Army in Multi-Domain Operations (Dec '18), for further information.

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).

Refer to FM 3-14 for doctrine on Army space operations.

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.

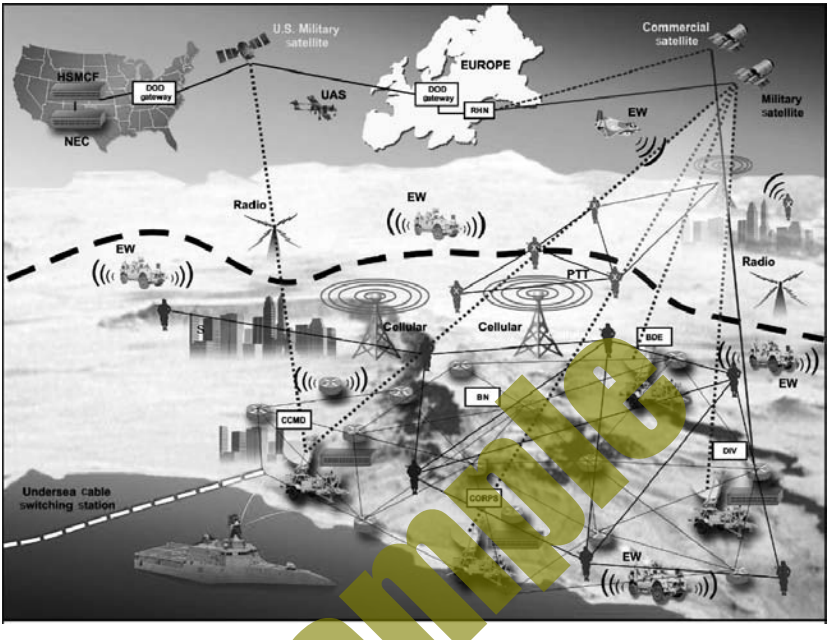
The information environment is comprised of three dimensions: physical, informational, and cognitive. The physical dimension includes the connective infrastructure that supports the transmission, reception, and storage of information.

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.

See following pages (pp. 0-10 to 0-11) for further discussion of the information environment, information as a joint function, and information operations.

Cyberspace and the Electromagnetic Spectrum

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.



Ref: FM 3-0 (Oct '17), fig. 1-2. Cyberspace in the multi-domain extended battlefield.

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.

Information Environment Operations (IEO)

The Joint Force seizes the initiative in competition by actively engaging in the information space across domains (to include cyberspace) and the EMS. The theater army converges Army actions and messaging in support of the Joint Force Commander's IEO, though all echelons engage in the information space in support of policy and commander's intent. To accomplish this mission, subordinate echelons must be enabled with access to intelligence, cyberspace, and EMS capabilities; appropriate authorities and permissions normally reserved for conflict or at higher echelons; and policy guidance expressed as intent rather than narrow, restrictive directives. This allows forward presence forces to aggressively take tailored actions and employ messages to counter and expose inconsistencies in the adversary's information warfare operations. The Army primarily contributes to the strategic narrative, however, by reinforcing the resolve and commitment of the U.S. to its partner and demonstrating its capabilities as a credible deterrent to conflict. *See also p. 1-9.*

TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations (Dec '18).

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.

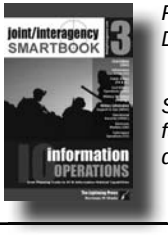
The **information function** encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making.

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 Joint/Interagency SMARTbook 3: Information Operations (Multi-Domain Guide to IO & Information-Related Capabilities), when published.

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.

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.

Influence Relevant Actors

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., KLE, CO, military information support operations [MISO], EW, CA) to reinforce the JFC's efforts. Since some relevant actors will be located outside of the JFC's OA, coordination, planning, and synchronization of activities with other commands or mission partners is vital.

Inform Domestic, International, and Internal Audiences

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.

Attack and Exploit Information, Information Networks, and Systems

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.

3. Support Human and Automated Decision Making

The management aspect of the information joint function includes activities that facilitate shared understanding across the joint force and that protect friendly information, information networks, and systems to ensure the availability of timely, accurate, and relevant information necessary for JFC decision making.

Facilitating Shared Understanding

Facilitating shared understanding is related to building shared understanding in the C2 joint function. Where building shared understanding is an element of C2 and focuses on purpose (i.e., the commander's objective), facilitating shared understanding is concerned with process (i.e., the methods). Key components of facilitating understanding are collaboration, KS, and IM.

Protecting Friendly Information

Information Networks, and Systems. The information function reinforces the protection function and focuses on protecting friendly information, information networks, and systems. This aspect of the information function includes the preservation of friendly information across the staff and the joint force and any information shared with allies and partners. These activities reinforce the requirement to assure the flow of information important to the joint force, both by protecting the information and by assessing and mitigating risks to that information. The preservation of information includes both passive and active measures to prevent and mitigate adversary collection, manipulation, and destruction of friendly information, to include attempts to undermine the credibility of friendly information.

CYBER1: The Cyberspace Operations & Electronic Warfare SMARTbook (Chapters)

Chap 1: Joint Cyberspace Operations (CO)

Most aspects of joint operations rely in part on cyberspace, which is the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Chap 2: Cyberspace Operations (OCO/DCO/DODIN)

Army cyberspace operations range from defensive to offensive. These operations establish and maintain secure communications, detect and deter threats in cyberspace to the DODIN, analyze incidents when they occur, react to incidents, and then recover and adapt while supporting Army and joint forces from strategic to tactical levels while simultaneously denying adversaries effective use of cyberspace and the electromagnetic spectrum (EMS). Cyberspace missions include DODIN operations, defensive CO, and offensive CO.

Chap 3: Electronic Warfare (EW) Operations

Electronic warfare refers to military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW capabilities enable Army forces to create conditions and effects in the EMS to support the commander's intent and concept of operations. EW includes EA, EP, and ES and includes activities such as electromagnetic jamming, electromagnetic hardening, and signal detection, respectively.

Chap 4: Cyber & EW (CEMA) Planning

The cyberspace planner is the subject matter expert to create effects in cyberspace and the EMS, with considerations from the CEMA section. Involving the cyberspace planner early in development of the commander's vision and planning allows for synchronization and integration with missions, functions, and tasks.

Chap 5: Spectrum Management Operations (SMO/JEMSO)

Spectrum management operations 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 JEMSO include all activities in military operations to successfully plan and execute joint or multinational operations in order to control the electromagnetic operational environment (EMOE).

Chap 6: DoD Info Network (DODIN) Operations

Department of Defense information network (DODIN) 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. DODIN operations are one of the three cyberspace missions.

Chap 7: Cybersecurity

The Army depends on reliable networks and systems to access critical information and supporting information services to accomplish their missions. Threats to the DODIN exploit the increased complexity and connectivity of Army information systems and place Army forces at risk. Like other operational risks, cyberspace risks affect mission accomplishment. Robust cybersecurity measures prevent adversaries from accessing the DODIN through known vulnerabilities.

Chap 8: Acronyms & Glossary

Chap 1

I. Joint Cyberspace Operations

Ref: JP 3-12, Cyberspace Operations (Jun '18), chap. I.

> *"... the United States (US) Department of Defense (DOD) is responsible for defending the US homeland and US interests from attack, including attacks that may occur in cyberspace. ... the DOD seeks to deter attacks and defend the US against any adversary that seeks to harm US national interests during times of peace, crisis, or conflict. To this end, the DOD has developed capabilities for cyberspace operations and is integrating those capabilities into the full array of tools that the US government uses to defend US national interests..."*
>
> *- The Department of Defense Cyber Strategy, April 2015*

I. Introduction

Most aspects of joint operations rely in part on **cyberspace**, which is the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

See following page (p. 1-2) for discussion of the nature of cyberspace.

JP 3-12 focuses on military operations in and through cyberspace; explains the relationships and responsibilities of the Joint Staff (JS), combatant commands (CCMDs), United States Cyber Command (USCYBERCOM), the Service cyberspace component (SCC) commands, and combat support agencies (CSAs); and establishes a framework for the employment of cyberspace forces and capabilities. Cyberspace forces are those personnel whose primary duty assignment is to a CO mission.

A. The Impact of Cyberspace on Joint Operations

Cyberspace capabilities provide opportunities for the US military, its allies, and partner nations (PNs) to gain and maintain continuing advantages in the operational environment (OE) and enable the nation's economic and physical security. 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.

Although it is possible for CO to produce stand-alone tactical, operational, or strategic effects and thereby achieve objectives, commanders integrate most CO with other operations to create coordinated and synchronized effects required to support mission accomplishment.

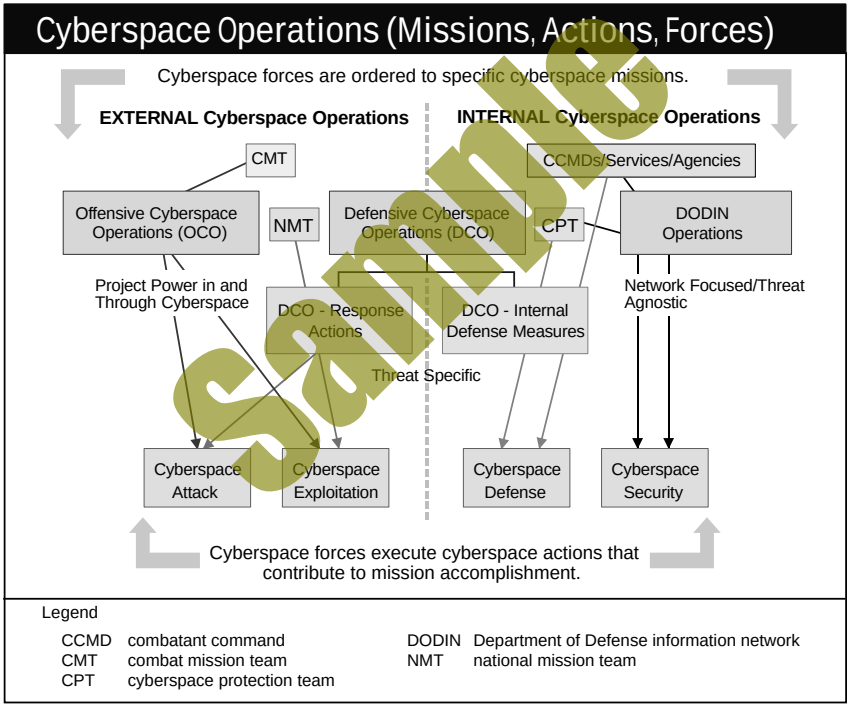
Military Operations In and Through Cyberspace

Ref: JP 3-12, Cyberspace Operations (Jun '18), pp. II-2 to II-9.

Referring to Adversary Activities in Cyberspace

DOD CO planning terms may not accurately describe the actions of our adversaries and enemies in cyberspace because their mission objectives and commander's intent may not be known with certainty. Therefore, the term "malicious cyberspace activity" refers to all such activities. If the context of the discussion requires more specific descriptions of this activity, use generic terms (e.g., attack, exploitation, sabotage, maneuver), depending upon the specific effects of the malicious actions.

Fig. II-1 below depicts the primary relationships between the cyberspace missions and actions. The depiction in Figure II-1 of the types of forces that normally conduct each type of CO mission is not intended to limit a JFC's ability to employ the best-qualified unit on any particular mission.



Ref: JP 3-12, Cyberspace Operations (Jun '18), fig. II-1. Cyberspace Operations Missions, Actions, and Forces.

Cyberspace MISSIONS

All actions in cyberspace that are not cyberspace-enabled activities are taken as part of one of three cyberspace missions: OCO, DCO, or DODIN operations. These three mission types comprehensively cover the activities of the cyberspace forces. The successful execution of CO requires integration and synchronization of these missions. Military cyberspace missions and their included actions are normally authorized by a military

order (e.g., execute order [EXORD], operation order [OPORD], tasking order, verbal order), referred to hereafter as mission order, and by authority derived from DOD policy memorandum, directive, or instruction. Cyberspace missions are categorized as OCO, DCO, or DODIN operations based only on the intent or objective of the issuing authority, not based on the cyberspace actions executed, the type of military authority used, the forces assigned to the mission, or the cyberspace capabilities used. Some orders may cover multiple types of missions.

See pp. 1-15 to 1-19 for discussion of cyberspace MISSIONS.

Cyberspace ACTIONS

Execution of any OCO, DCO, or DODIN operations mission requires completion of specific tactical-level actions or tasks that employ cyberspace capabilities to create effects in cyberspace. All cyberspace mission objectives are achieved by the combination of one or more of these actions, which are defined exclusively by the types of effects they create. To plan for, authorize, and assess these actions, it is important the commander and staff clearly understand which actions have been authorized under their current mission order. For example, the transition from DODIN operations to DCO-IDM missions may need to occur quickly whenever the DODIN is threatened and cyberspace operators begin to take cyberspace defense actions. To enable and synchronize this transition and subsequent cyberspace defense actions, clear orders are required that communicate to cyberspace operators the applicable constraints, restraints, and authorities. Since they will always be necessary, standing orders for DODIN operations and DCO-IDM missions cover most cyberspace security and initial cyberspace defense actions. However, OCO and DCO-RA missions are episodic. They may require clandestine maneuver and collection actions or may require overt actions, including fires. Therefore, the approval for CO actions in foreign cyberspace requires separate OCO or DCO-RA mission authorities.

See pp. 1-20 to 1-22 for discussion of cyberspace ACTIONS.

National Intelligence Operations In and Through Cyberspace

National-level intelligence organizations conduct intelligence activities in, through, and about cyberspace in response to national intelligence priorities. This intelligence can support a military commander's planning and preparation. Although DOD's cyberspace forces may collect tactically and operationally useful information while maneuvering to and through foreign cyberspace, like all joint forces, they also depend on intelligence support from traditional military and national intelligence sources.

Department of Defense Ordinary Business Operations In and Through Cyberspace

Ordinary business operations in and through cyberspace are "cyberspace-enabled activities" that comprise those non-intelligence and non-warfighting capabilities, functions, and actions used to support and sustain DOD forces and components. This includes the cyberspace-enabled functions of the civilian-run DOD agencies and activities, such as the Defense Finance and Accounting Service and the Defense Contract Audit Agency. Since the conduct of DOD ordinary business operations in cyberspace is guided by DOD policy and not generally by joint doctrine, it is not discussed here in detail. However, vulnerabilities that may exist in the applications and devices used for DOD ordinary business operations might be exploited in a manner that directly impacts a military commander's mission. Since DOD agencies and activities use many of the same networks as military commanders, a compromise in any area of the DODIN used for business operations might result in a loss of mission assurance in cyberspace for military operations.

III. Authorities, Roles, & Responsibilities

Ref: JP 3-12, Cyberspace Operations (Jun '18), chap. III.

> *"The Defense Department (DOD) requires the commitment and coordination of multiple leaders and communities across DOD and the broader US [G] government to carry out its missions and execute this strategy. Defense Department law enforcement, intelligence, counterintelligence, and policy organizations all have an active role, as do the men and women that build and operate DOD's networks and information technology systems. Every organization needs to play its part."*
>
> *- Ashton B. Carter Secretary of Defense, The Department of Defense Cyber Strategy, April 17, 2015*

I. Introduction

Under the authorities of SecDef, DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation. USCYBERCOM coordinates with CCMDs, the JS, and the Office of the Secretary of Defense (OSD); liaises with other USG departments and agencies; and, in conjunction with DHS, DOD's DC3, and the Defense Security Service, liaises with members of the DIB. Similarly, as directed, DOD deploys necessary resources to support efforts of other USG departments and agencies, and allies.

The National Military Strategy and The Department of Defense Cyber Strategy provide high-level requirements for national defense in cyberspace and DOD's role in defending DOD and larger US national security interests through CO.

DOD's Roles and Initiatives in Cyberspace

DOD's roles in cyberspace are, for the most part, the same as they are for the physical domains. As a part of its role to defend the nation from threats in cyberspace, DOD prepares to support DHS and the Department of Justice (DOJ), the USG leads for incident response activities during a national cybersecurity incident of significant consequences. To fulfill this mission, DOD conducts military operations to defend DOD elements of CI/KR and, when ordered, defend CI/KR related to vital US interests. DOD's national defense missions, when authorized by Presidential orders or standing authorities, take primacy over the standing missions of other departments or agencies. The Department of Defense Cyber Strategy establishes strategic initiatives that offer a roadmap for DOD to operate effectively in cyberspace, defend national interests, and achieve national security objectives.

National Incident Response

When directed, DOD provides cyberspace defense support during major cyberspace threat events to the US. DOD coordinates with the requesting agency or department through the lead response department or agency, as described in the Presidential Policy Directive (PPD)-41, United States Cyber Incident Coordination. When DHS requests such support, the fundamental principles of DSCA used to respond to domestic emergencies in the physical domains also apply to CO support.

United States Code

Ref: JP 3-12, Cyberspace Operations (Jun '18), fig. III-1, p. III-3.

United States Code (USC)	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of US cyberspace
Title 10	*Armed Forces*	National defense	Department of Defense	Man, train, and equip US forces for military operations in cyberspace
Title 18 Title 28	*Crimes and Criminal Procedure* *Judiciary and Judicial Procedure*	Law enforcement	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	*National Guard*	National defense and civil support training and operations, in the US	State Army National Guard, State Air National Guard	Domestic consequence management (if activated for federal service, the National Guard is integrated into the Title 10, USC), *Armed Forces*
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All Federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies
Title 44	*Public Printing and Documents*	Defines basic agency responsibilities and authorities for information security policy	All Federal departments and agencies	The foundation for what we now call cybersecurity activities, as outlined in Department of Defense Instruction, 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations*.
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the Department of Defense and intelligence community agencies aligned under the Office of the Director of National Intelligence	Secure US interests by conducting military and foreign intelligence operations in cyberspace

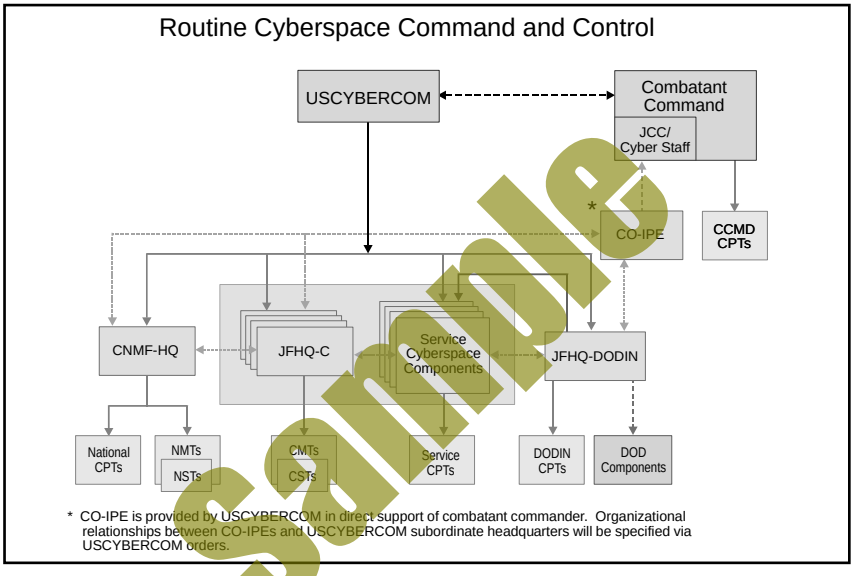
C2 Distinctives for Routine and Crisis/Contingency CO

Ref: JP 3-12, Cyberspace Operations (Jun '18), pp. IV-12 to IV-15.

The CJCS has established two models for C2 of CO, depending upon the prevailing circumstances. The relationships are described below and depicted graphically in Figure IV-1 and Figure IV-2.

Routine CO

The following relationships guide the C2 of cyberspace forces during normal operating conditions, when no crisis or contingency is in effect:



Ref: JP 3-12, Cyberspace Operations (Jun '18), fig. IV-1. Routine Cyberspace Command and Control.

USCYBERCOM C2 Relationships

1. CDRUSCYBERCOM has COCOM of all GFMIG-assigned cyberspace forces.
2. CDRUSCYBERCOM has support relationships with all other CCDRs.
3. CNMF commander has OPCON of NMTs/NSTs and national CPTs.
4. JFHQ-C commanders have OPCON of CMTs/CSTs.
5. SCC commanders have OPCON of Service CPTs and other forces attached by CDRUSCYBERCOM (e.g., CSSPs).
6. JFHQ-DODIN commander has OPCON of DODIN CPTs.
7. JFHQ-DODIN commander has tactical control (TACON) of SCC commands for DODIN operations and DCO-IDM only.
8. JFHQ-DODIN commander has DACO, delegated from CDRUSCYBERCOM, over all DOD components for global DODIN operations and DCOIDM.
9. SCC commanders have DACO, delegated from CDRUSCYBERCOM, over all related Service components for DODIN operations and DCO-IDM.

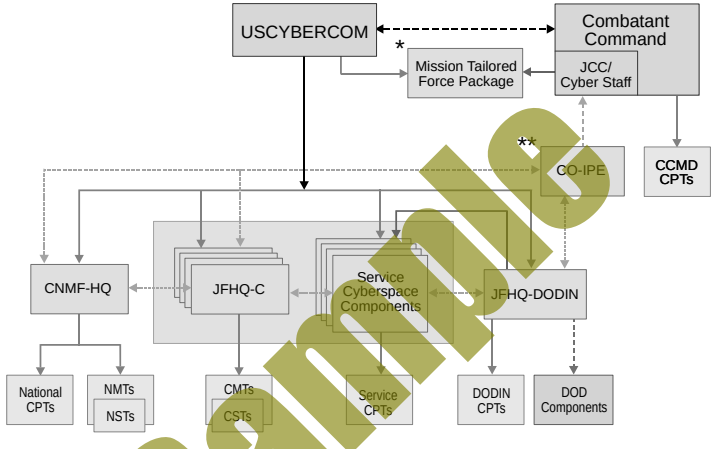
CCMD C2 Relationships

1. CCDRs have COCOM of assigned cyberspace forces.
2. CCDRs have OPCON of CCMD CPTs.
3. SecDef establishes support relationships between CCDRs for CO.
4. JFHQ-C commanders support more than one CCDR using the general support model.
5. USCYBERCOM CO-IPEs provide direct support to CCDRs.

Crisis / Contingency CO

When a cyberspace-related crisis or contingency is in effect, the routine relationships carry over, with these additional caveats:

Crisis/Contingency Cyberspace Command and Control



* USCYBERCOM Commander has OPCON of the mission-tailored force package and retains the flexibility to delegate OPCON to subordinate headquarters depending on the nature of the crisis/contingency. The commander receiving a mission-tailored force package has TACON to control the timing and tempo of cyberspace operations.

**Organizational relationships between CO-IPEs and USCYBERCOM subordinate headquarters will be specified via USCYBERCOM orders.

1. USCYBERCOM commander retains OPCON of any cyberspace forces USCYBERCOM provides to support a CCDR for crisis/contingency operations.
2. When directed, CCDRs receiving forces from USCYBERCOM for crisis/contingency operations (e.g., a mission-tailored force package [MTFP]) have TACON of those forces.

Legend (Figures IV-1 and IV-2)

CCMD	combatant command
CMT	combat mission team
CNMF-HQ	Cyber National Mission Force Headquarters
COCOM	combatant command (command authority)
CO-IPE	cyberspace operations-integrated planning element
CPT	cyberspace protection team
CST	combat support team
DACO	directive authority for cyberspace operations
DOD	Department of Defense
DODIN	Department of Defense information network
JCC	Joint Cyber Center
JFHQ-C	joint force headquarters-cyberspace
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
NMT	national mission team
NST	national support team
OPCON	operational control
TACON	tactical control
USCYBERCOM	United States Cyber Command

COCOM
OPCON
TACON
DACO
supporting/supported
direct support
coordination

I(a). Cyberspace and the Electromagnetic Spectrum

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), chap. 1.

Superiority in cyberspace and the electromagnetic spectrum (EMS) provides a decisive advantage to commanders at all levels in modern combat. The Army's ability to exploit cyberspace and EW capabilities will prove critical to the success of unified land operations. As cyberspace and EW operations develop similar and complementary capabilities, the Army must plan, integrate, and synchronize these operations with unified land operations.

Employing cyberspace and EW capabilities under a single planning, integration, and synchronization methodology increases the operational commander's ability to understand the environment, project power, and synchronize multiple operations using the same domain and environment. Synchronizing offensive and defensive activities allows a faster response to enemy and adversary actions. The EMS is the common denominator for both cyberspace and EW operations, and also impacts every operation in the Army.

The distinctions between cyberspace and EW capabilities allow for each to operate separately and support operations distinctly. However, this also necessitates synchronizing efforts to avoid unintended interference. Any operational requirement specific to electronic transfer of information through the wired portion of cyberspace must use a cyberspace capability for affect. If the portion of cyberspace uses only the EMS as a transport method, then it is an EW capability that can affect it. Any operational requirement to affect an EMS capability not connected to cyberspace must use an EW capability.

The Department of Defense information network-Army (DODIN-A) is the Army's critical warfighting platform, which enables mission command, precision fires, intelligence, logistics, and tele-medicine, and supports all operations. Access to the DODIN-A allows commanders to project combat power, conduct support operations, and achieve joint and Army force commander objectives. Securing and operating this expansive network is one of the most complex and important operations the Army currently undertakes. A single vulnerability within this network can place units and operations at risk, potentially resulting in mission failure. Understanding how to operationalize cyberspace and the EMS is a fundamental staff proficiency and commander's priority.

Superiority in cyberspace and the EMS to support Army operations results from effectively synchronizing Department of Defense information network (DODIN) operations, offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), electronic attack, electronic protection, electronic warfare support, and spectrum management operations (SMO). 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). Through CEMA, the Army plans, integrates, and synchronizes these missions, supports and enables the mission command system, and provides an interrelated capability for information and intelligence operations.

Cyberspace and the EMS will likely grow increasingly congested, contested, and critical to successful unified land operations. Success will be measured by the ability to execute operations freely in cyberspace and the EMS, while controlling the ability of others to operate in the domain.

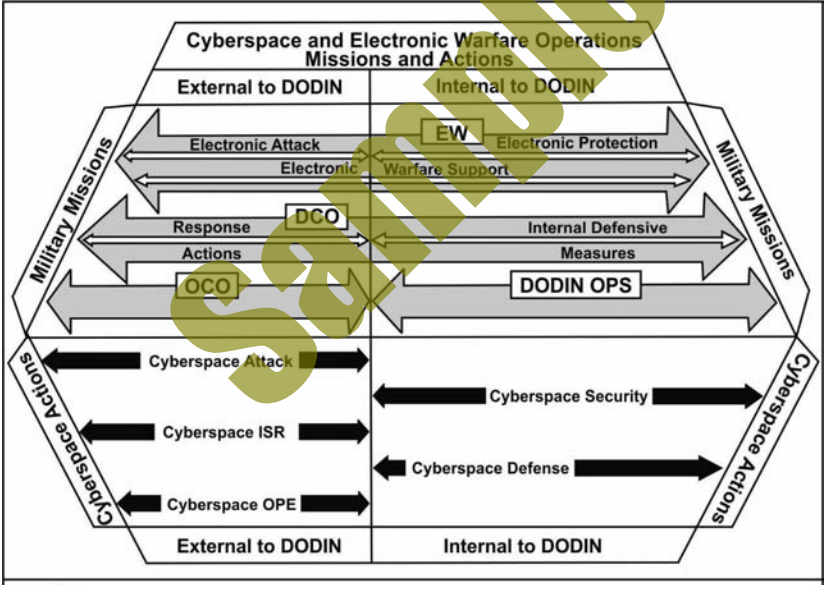
See following page (p. 2-2) for a discussion of the cyberspace domain.

Cyberspace Missions and Actions

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), pp. 1-6 to 1-7.

Cyberspace missions and actions are interrelated; synchronizing and supporting efforts among the cyberspace missions is imperative to maintaining freedom of maneuver in cyberspace. Supporting the cyberspace missions are the cyberspace actions: cyberspace defense; cyberspace intelligence, surveillance, and reconnaissance (ISR); cyberspace OPE; cyberspace attack; and cyberspace security. Cyberspace actions support DODIN operations, DCO, OCO, or any combination thereof. Executing cyberspace actions at any echelon is dependent on authority, capability, and coordination. The actions are interrelated and a cyberspace mission may require more than one action to achieve mission success.

Army forces can execute cyberspace missions and actions under the proper authority. Since DODIN operations and some DCO tasks may overlap, Army forces may conduct multiple cyberspace missions or actions as part of their daily duties and responsibilities. Situational requirements may dictate the transition from cyberspace security to DCO internal defensive measures (DCO-IDM). Figure 1-3 below shows the relationship of the cyberspace missions and cyberspace actions both external and internal to the DODIN and the owned, leased, shared partner portions of cyberspace. EW can affect the cyberspace capabilities that use the EMS.



Ref: FM 3-12 (Apr '17), 1-3. Cyberspace and electronic warfare operations -missions and actions.

Use of the DODIN relies upon DODIN operations, DCO, and at times on OCO for freedom of maneuver to employ a network capability. Cyberspace security and DCO protect and defend Army networks, thereby maintaining communications and mission command. Current intrusion information may lead to future defensive cyberspace operations response action (DCO-RA) or OCO missions. DCO and OCO depends on the DODIN for planning, synchronization, and integration of missions. EW may also support and enable cyberspace operations through electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

V. Effects Outside of DODIN and Cyberspace

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), pp. 1-10 to 1-11.

Effects delivered in and through cyberspace manifest in cyberspace or in one or more of the other domains. The Army requests effects in cyberspace after planning and targeting activities. The effects may be delivered by or through an OCO or DCO-RA mission. The effects support Army operations and JFC objectives. Cyber mission forces conducting cyberspace actions deliver effects in and through cyberspace. EW capabilities can be a conduit to deliver effects in and through cyberspace. Joint organizations express the effects in cyberspace in different terms than expressed in the traditional Army targeting methodology. Army targeting efforts result in requirements using Army terms similar in meaning to joint cyberspace terms. However, the difference in terms requires that any requests from echelons corps and below to joint organizations use the joint terms for effects in cyberspace.

Cyberspace Actions

Joint cyberspace operations doctrine describes cyberspace actions. Cyberspace actions at the joint level require creating various direct denial effects in cyberspace (degradation, disruption, or destruction). Joint cyberspace operations doctrine also explains that manipulation leads to denial (hidden or manifesting) in any domain.

These specific actions are—

Deny

To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents enemy or adversary use of resources.

Degrade

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

Disrupt

To completely but temporarily deny (a function of time) 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 selected is 100 percent.

Destroy

To permanently, completely, and irreparably deny (time and amount are both maximized) access to, or operation of, a target.

Manipulate

To control or change the enemy or adversary's information, information systems, and/or networks in a manner that supports the commander's objectives.

Effects

Army commanders request effects using the terms deny, degrade, disrupt, destroy, and manipulate. The Army considers these as separate effects rather than a subset of deny. These terms are common for targeting guidance or to describe effects for information operations (IO). These are desired effects that support operations and are achievable using cyberspace capabilities. Army planners will utilize these terms to describe and plan for cyberspace and electronic warfare effects. The most common effects associated with cyberspace operations are deny, degrade, disrupt, destroy, and manipulate.

For more effects or information on effects refer to ATP 3-60.

Denial

Denial operations are actions to hinder or deny the enemy the use of space, personnel, supplies, or facilities (FM 3-90-1). An example of deny is to use EW capabilities to jam specific frequencies using an EW capability for a predetermined amount of time, or to block a router communication port using cyberspace capability for some predetermined amount of time; however, the duration of denial will depend on the enemy's ability to reconstitute.

Degrade

Degrade is to use nonlethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems and information collections efforts or means. An example of degrade is slowing the cyberspace connection speed affecting the ability to effectively communicate or pass data in a timely manner.

Disrupt

Disrupt is a tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt the enemy's timetable, or cause enemy forces to commit prematurely or attack in a piecemeal fashion. An obstacle effect that focuses fires planning and obstacle efforts to cause the enemy force to break up its formation and tempo, interrupt its timetable, commit breaching assets prematurely, and attack in a piecemeal effort (FM 3-90-1). An example of disrupt is interrupting the connection to cyberspace, either wired or wireless, affecting the ability to communicate or pass data.

Destroy

Destroy is tactical mission task that physically renders an enemy force combat-ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt (FM 3-90-1). Destroy is applying lethal combat power on an enemy capability so that it can no longer perform any function. The enemy cannot restore it to a usable condition without being completely rebuilt. An example of destroy using cyberspace capabilities is causing a system to lose all of its operating information or causing it to overheat to a point it is no longer usable.

Manipulate

Manipulate is to control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives. The Army uses the same description as the joint cyberspace action for this effect.

Deceive

Deceive is when military leaders attempt to mislead threat decision makers by manipulating their understanding of reality. An example of deceive is modifying a message causing the enemy or adversary to assemble in a location not originally designated by their own chain of command.

Effects in and through cyberspace may have the same consequences as other types of traditional effects. Effects during operations include lethal and non-lethal actions and may be direct or indirect. Direct effects are first order consequences and indirect effects are second, third, or higher order consequences. Similar characteristics of direct and indirect effects in cyberspace can be cumulative or cascading if desired. These effects are planned and controlled in order to meet the commander's objectives. Cumulative refers to compounding effects and cascading refers to influencing other systems with a rippling effect. The desired effects in cyberspace can support operations as another means to shape the operational environment to provide an advantage.

Refer to JP 3-60 for more information on cascading and cumulative effects.

VIII. Threats in Cyberspace

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), table 1-1, p. 1-21.

The Army faces multiple, simultaneous, and continuous threats in cyberspace. A threat is any combination of actors, entities, or forces that have the capability and intent to harm the United States forces, United States national interests, or the homeland (ADRP 3-0). Threats include state and non-state actors, criminals, insider threats, and the unwitting individuals who intend no malice. These diverse threats have disparate agendas, alliances, and range of capabilities. Enemies and adversaries employ regular and irregular forces and use an ever-changing variety of conventional and unconventional tactics. Risks from insiders may be malicious or cause damage unintentionally. Insider risks include non-compliance of policies and regulations, causing vulnerabilities on the network. Table 1-1 below lists sample threat capabilities with examples of methods, indicators, and first order effects.

Capability	*Methods*	*Indicators*	*First-Order Effects*
Denial of service attack	Overwhelming a web service, server, or other network node with traffic to consume resources preventing legitimate traffic	Abnormal network performance, inability to navigate web and access sites, uncontrolled spam, and system reboots	Degraded network capabilities ranging from limited operational planning to total denial of use
Network penetration	Man-in-the-middle attacks, phishing, poisoning, stolen certificates, and exploiting unencrypted messages and homepages with poor security features	Unfamiliar e-mails, official looking addresses requiring urgent reply, internet protocol packets replaced, non-legitimate pages with the look of legitimate sites, directed moves from site to site, requests to upgrade and validate information, and unknown links	Uncontrolled access to networks, manipulation of networks leading to degraded or compromised capabilities that deny situational awareness or theft of data
Emplaced malware (virus, worms spyware, and rootkits)	Phishing, spear-phishing, pharming, insider threat introduction, open-source automation services, victim activated through drive-by downloads and victim emplaced data storage devices	Pop-ups, erroneous error reports, planted removable storage media, unknown e-mail attachments, changed passwords without user knowledge, automatic downloads, unknown apps, and degraded network	Spyware and malware on affected systems allow electronic reconnaissance, manipulation, and degrading system performance
Disrupt or deny information systems in the EMS	Prevent friendly antennas from receiving data transmitted in the EMS by using military or commercially available high-powered lasers, high powered microwaves, and repurposed or re-engineered communications systems	Symptoms may not be evident if passive; may manifest as transmission interference, software or hardware malfunctions, or the inability to transmit data	Degraded or complete denial of service in ability to control the EMS denying situational awareness and degrading operational planning

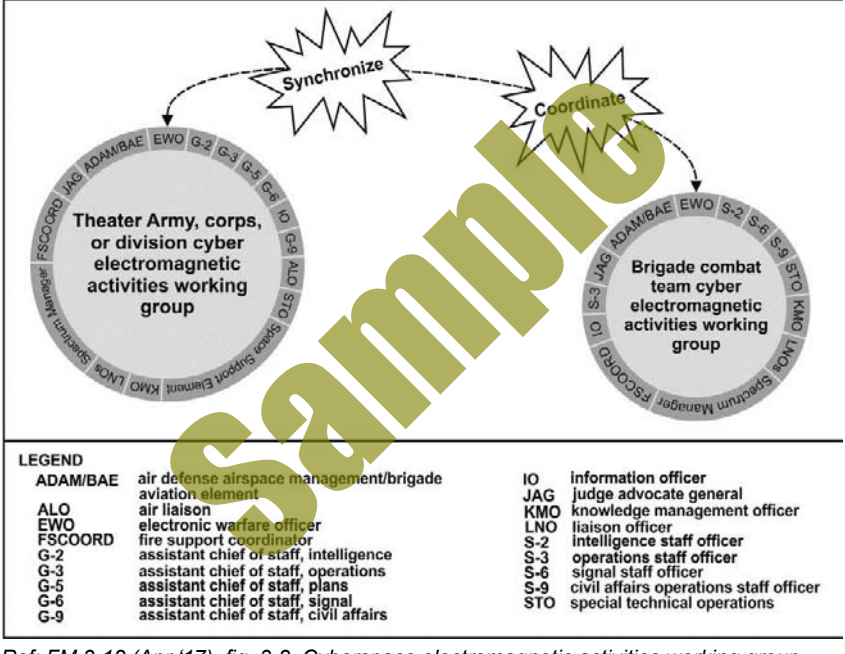
Ref: FM 3-12 (Apr '17), Table 1-1. Sample cyberspace and electronic warfare threat capabilities. See pp. 7-16 to 7-18 for discussion of cyber threat activities and pp. 7-18 to 7-19 for an overview and discussion of cyber attack tools.

C. Cyberspace Electromagnetic Activities (CEMA) Working Group

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), pp. 3-10 to 3-13.

The CEMA working group is accountable for integrating cyberspace and EW operations and related actions into the concept of operations. CEMA working groups do not add additional structure to an existing organization. The CEMA working group is led by the EWO to analyze, coordinate, and provide recommendations for a particular purpose, event, or function. Deletions or modifications to the CEMA working group staff are based on requirements. Figure 3-2 below outlines the functions of the CEMA working group. The CEMA working group augments the function of the staff executing CEMA.

CEMA Working Group Organization



Ref: FM 3-12 (Apr '17), fig. 3-2. Cyberspace electromagnetic activities working group organization.

Roles in the Cyberspace Electromagnetic Activities (CEMA) Working Group

The CEMA working group is responsible for coordinating horizontally and vertically to support unified land operations and will primarily deconflict detection and delivery assets through the planning and targeting processes. Staff representation within the CEMA working group may include the G-2 (S-2), G-3 (S-3), G-6 (S-6), assistant chief of staff, civil affairs operations G-9 (S-9), fire support coordinator, IO officer, space support element, legal advisor, and a joint terminal attack controller when assigned. Deletions or modifications to the CEMA working group staff are based on requirements for certain capabilities and assets.

CEMA Working Group (Participants and Functions)

Participants	CEMA Working Group Functions
Division and above Airspace Management /brigade aviation element ALO EWO G-2 G-3 G-5 G-6 G-9 IO Officer FSCOORD JAG KMO LNOs Spectrum manager Space support element STO	■ Plan, integrate, and synchronize cyberspace and EW operations to support operations or command requirements. ■ Plan and nominate targets within cyberspace and the EMS to achieve effects that support the commander's intent. ■ Develop and integrate cyberspace and EW operations actions into operations plans and operational concepts. ■ Develop information to support planning (joint restricted frequency list, spectrum management, and deconfliction). ■ Develop and promulgate CEMA policies and support higher-level policies. ■ Identify and coordinate intelligence support requirements for CEMA. ■ Maintain current assessment of resources available to the commander for cyberspace and EW operations. ■ Prioritize effects and targets for functions and capabilities within cyberspace and the EMS. ■ Predict effects of friendly and enemy cyberspace and EW operations. ■ Plan and submit measures of performance and effectiveness information requirements to intelligence section. ■ Identify the measures of effectiveness for cyberspace and EW operations. ■ Coordinate spectrum management and radio frequency deconfliction with G-6 and J-6. ■ Plan, assess, and implement friendly electronic security measures. ■ Ensure cyberspace and EW operations actions comply with applicable policy and laws. ■ Identify civilian and commercial cyberspace and EW operations related capacity and infrastructure within the area of operations.
Brigade ADAM/BAE ALO EWO FSCOORD JAG KMO S-2 S-3 S-6 S-9 IO Officer LNOs Spectrum manager	■ Develop and integrate cyberspace and EW actions into operation plans and exercises. ■ Support CEMA policies. ■ Plan, prepare, execute, and assess cyberspace and EW operations. ■ Integrate intelligence preparation of the battlefield into the operations process. ■ Identify and coordinate intelligence support requirements for BCT and subordinate units' cyberspace and EW operations. ■ Assess offensive and defensive requirements for cyberspace and EW operations. ■ Maintain current assessment of cyberspace and EW resources available to the unit. ■ Nominate and submit approved targets within cyberspace to division. ■ Prioritize BCT targets within cyberspace and the EMS. ■ Plan, coordinate, and assess friendly CEMA. ■ Implement friendly electronic and network security measures (for example, electromagnetic spectrum mitigation and network protection). ■ Ensure cyberspace and EW operations actions comply with applicable policy and laws. ■ Identify civilian and commercial cyberspace and EMS-related capacity and infrastructure within the area of operations.

ADAM/BAE air defense airspace management/brigade aviation element operations
ALO air liaison officer
BCT brigade combat team
CEMA cyberspace electromagnetic activities staff
EMS electromagnetic spectrum
EW electronic warfare
EWO electronic warfare officer
FSCOORD fire support coordinator
G-2 assistant chief of staff, intelligence
G-3 assistant chief of staff, operations
G-5 assistant chief of staff, plans
G-6 assistant chief of staff, signal
G-9 assistant chief of staff, civil affairs
IO information operations
JAG judge advocate general
J-6 communications directorate of a joint
KMO knowledge management officer
LNO liaison officer
NCO noncommissioned officer
STO special technical operations
S-2 intelligence staff officer
S-3 operations staff officer
S-6 signal staff officer
S-9 civil affairs officer

Ref: FM 3-12 (Apr '17), table 3-1. Tasks of the cyberspace electromagnetic activities working group.

Chap 3

I. Electronic Warfare Operations

Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), pp. 1-25 to 1-35.

I. Electronic Warfare (EW)

Electronic warfare refers to military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). EW capabilities enable Army forces to create conditions and effects in the EMS to support the commander's intent and concept of operations.

Electronic Warfare (EW) Operations

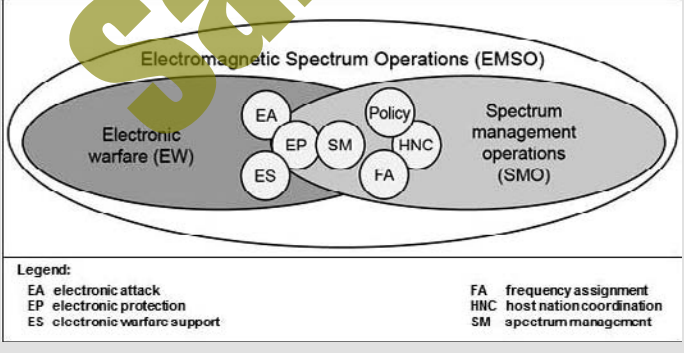
A **Electronic Attack (EA)**

B **Electronic Protection (EP)**

C **Electronic Warfare Support (ES)**

Electromagnetic Spectrum Operations (EMSO)

EMSO are comprised of EW and 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.



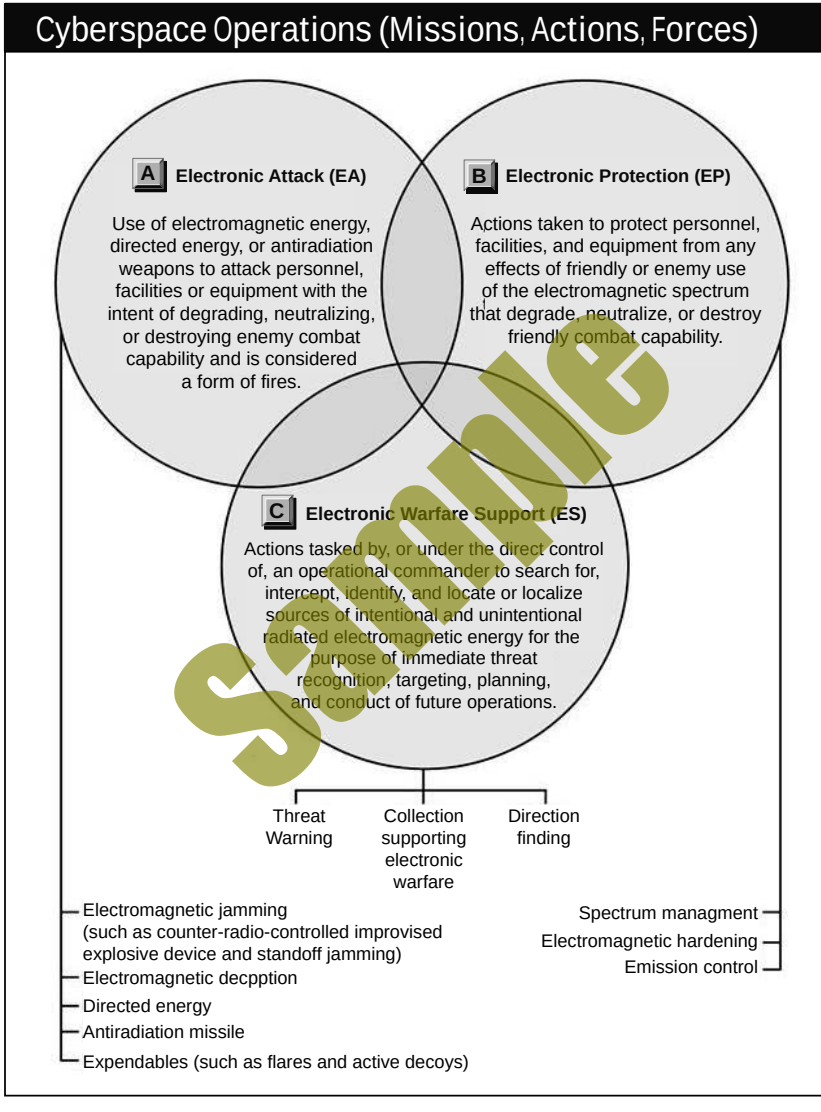
Ref: FM 3-12 (Apr '17), fig. 1-8. Electromagnetic spectrum operations.

Throughout this document, the term EW operations refers to planning, preparing, execution, and continuous assessment of the electronic warfare activities of an operation. The term EMSO indicates the addition of those operationally related spectrum management operations activities.

II. Electronic Warfare Missions

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), fig. 1-9.

With proper integration and deconfliction, EW can create reinforcing and complementary effects by affecting devices that operate in and through wired and wireless networks.



Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), fig. 1-9. Electronic warfare missions.

Electronic Protection Actions

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), pp. 1-29 to 1-30.

There are several actions related to EP. They include—

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 3-13.1). It involves the application of sound EMS management; system, equipment, and device design configuration that ensures interference-free operation. It also involves clear concepts and doctrines that maximize operational effectiveness.

Electromagnetic Hardening

Electromagnetic hardening consists of action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (JP 3-13.1). Electromagnetic hardening is accomplished by using a comprehensive shielding of sensitive components and by using non-electrical channels for the transfer of data and power.

Electromagnetic Spectrum Management

Electromagnetic spectrum management is planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures (JP 6-01). The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

Electronic Masking

Another task of electronic protection is electronic masking. Electronic 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 electronic warfare support measures/SIGINT without significantly degrading the operation of friendly systems (JP 3-13.1).

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 3-13.1). Emission control prevents the enemy from detecting, identifying, and locating friendly forces. It is also used to minimize electromagnetic interference among friendly systems.

Wartime Reserve Modes

Wartime reserve modes are characteristics and operating procedures of sensors, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance (JP 3-13.1). Wartime reserve modes are deliberately held in reserve for wartime or emergency use and seldom employed outside of conflict.

Chap 3

II. EW Divisions & Key Personnel

Ref: ATP 3-36, Electronic Warfare Techniques (Dec '14), pp. 1-3 to 1-11.

I. Key Personnel for Planning and Coordinating Electronic Warfare Activities

Key personnel involved in the planning and coordination of EW activities are—

- G-3 (S-3) staff
- Electronic warfare officer
- G-2 (S-2) staff
- Network operations officer
- Spectrum manager
- Information operations officer
- Staff judge advocate or representative
- Electronic warfare control authority

Other key personnel involved in the planning and coordination of EW activities include—

- Fire support coordinator
- G-5 (S-5) staff
- G-6 or S-6 staff
- Liaison officers
- Space support element
- Special technical operations staff

A. G-3 (S-3) Staff

The G-3 (S-3) staff is responsible for the overall planning, coordination, and supervision of EW activities, except for intelligence. 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 actions to assigned and attached units.
- Exercises control over EA, including integration of electromagnetic deception plans.
- Directs EP measures the unit will take based on recommendations from the G-6 (S-6), the electronic warfare officer, and the CEMA working group.
- Coordinates and synchronizes EW training with other unit training requirements.
- Issues EW support tasks within the unit information collection plan. These tasks are according to the collection plan and the requirements tools developed by the G-2 (S-2) and the requirement manager.
- Coordinates with the CEMA working group to ensure planned EW operations support the overall tactical plan.
- Integrates EA within the targeting process.

Electronic Warfare Element (EWE) Personnel

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), pp. 1-8 to 1-9.

The EWE has the following personnel: electronic warfare officer, electronic warfare technician, electronic warfare noncommissioned officer, and spectrum manager.

Electronic Warfare Officer (29A)

The electronic warfare officer (29A) —

- Serves as the commander's subject matter expert and advisor on all EW matters.
- Plans, coordinates, synchronizes, and deconflicts EW tasks to support unified land operations.
- Integrates EW intelligence preparation of the battlefield (IPB) into the military decisionmaking process (MDMP).
- Provides input to fragmentary orders for EW tasks to support unified land operations.
- Identifies the potential for frequency fratricide in the MDMP.
- Plans, coordinates, and synchronizes EW activities and assets into unified land operations.
- Recommends priorities for EW effects and targets, and integrates EW into the targeting process.
- Coordinates, synchronizes, and deconflicts with collection manager and G-2 (S-2).
- Coordinates and reviews EW battle damage assessment.
- Coordinates CEMA in units conducting cyberspace operations.
- Maintains current assessment of EW resources available.
- Leads the CEMA working group.
- When designated, serves as the electronic warfare control authority.
- Supervises and manages EW activities for the commander.
- Oversees the creation of all EW products for dissemination.

Electronic Warfare Technician (290A)

The electronic warfare technician (290A) —

- Serves as the technical subject matter expert for EW to the EWO and CEMA working group.
- Plans, coordinates, and assesses EW offensive, defensive, and support requirements.
- Provides input to the integration of enemy electronic threat characteristics information into IPB.
- Provides subject matter expertise on technical and tactical employment of EW systems.
- Integrates EW in the targeting process, monitors EW target requests, and conducts battle damage assessments.
- Plans and coordinates EW operations across functional and integrating cells.
- Recommends employment and operation of available EW assets and maintains current resource status for CEMA working group.

- Provides technical oversight and supervision of the maintenance of EW equipment.
- Plans, manages, and executes EW collective tasks.
- Incorporates EW assets and plans into the collection and targeting staff processes.
- Develops EW products for inclusion into the targeting process.
- Facilitates CEMA working group efforts.
- Conducts, maintains, and updates an electromagnetic energy survey.
- Identifies EW enemy and friendly effects in the ES.
- Coordinates, synchronizes, and deconflicts with collection manager and G-2 (S-2).
- Ensures the EWO has all pertinent EW information to maintain situational awareness (maintains EW smart book, follows standard operating procedures, and briefs EWO as needed).

Electronic Warfare Noncommissioned Officer (29E)

The electronic warfare noncommissioned officer (NCO) (29E) —

- Plans, manages, and executes EW individual tasks.
- Conducts organic and nonorganic EW asset visibility and management.
- Serves as senior developer and trainer for EW tasks.
- Distributes, maintains, and consolidates EW products.
- Conducts all administrative actions for CEMA working group.
- Collects logs and data for electromagnetic energy surveys.
- Coordinates and deconflicts with 25E (spectrum manager).
- Coordinates, synchronizes, and deconflicts with collection manager and G-2 (S-2).
- Manages the EW current operations situational awareness.
- Ensures all subordinate EW personnel maintain proficiency and adequately support their assigned unit.

Spectrum Manager (25E)

The spectrum manager (25E) —

- Assists with mitigation of offensive and defensive EA on friendly emitters.
- Provides input to the ES plan.
- Conducts analysis of EW requests to determine impact on friendly emitters and recommend mitigation.
- Issues the signal operating instructions.
- Provides all spectrum resources to the task force.
- Coordinates the preparation of the joint restricted frequency list and issuance of emissions control guidance.
- Coordinates electromagnetic deception plans and operations in which assigned communications resources participate.
- Coordinates measures to eliminate, moderate, or mitigate electromagnetic interference.
- Coordinates with higher echelon spectrum managers for electromagnetic interference resolution that cannot be resolved internally.
- Assists the EWO in issuing guidance in the unit (including subordinate elements) regarding deconfliction and resolution of interference problems between EW systems and other friendly systems.

I. Electronic Attack (EA) Considerations

Ref: ATP 3-36, Electronic Warfare Techniques (Dec '14), pp. 2-8 to 2-10.

EA includes both offensive and defensive activities. These activities differ in their purpose. Offensive EA denies, disrupts, or destroys enemy capability. Defensive EA protects friendly personnel and equipment or platforms. In either case, certain considerations are involved in planning for employing EA, such as—

- Friendly communications.
- Information collection.
- Other effects.
- Electromagnetic spectrum use by local, nonhostile parties.
- Hostile intelligence collection.
- Persistency of effect.

The EWO, the G-2 (S-2), the G-3 (S-3), the G-6 (S-6), the spectrum manager, and the information operations officer coordinate closely to avoid friendly communications interference that can occur when using EW systems on the battlefield. Coordination ensures that EA system frequencies are properly deconflicted with friendly communications and intelligence systems, or that ground maneuver and friendly information tasks are modified accordingly.

The number of information systems, EW systems, and sensors operating simultaneously on the battlefield makes deconfliction with communications systems a challenge. The EWO, the G-2 (S-2), the G-6 (S-6), and the spectrum manager plan and rehearse deconfliction procedures to adjust their use of EW or communications systems quickly.

EA operations depend on ES and SIGINT to provide targeting information and battle damage assessment. However, EWOs must keep in mind that not all information collection focuses on supporting EW. If not properly coordinated with the G-2 (S-2) staff, EA operations may interrupt information collection by jamming or inadvertently interfering with a particular frequency being used to collect data on the threat or by jamming a given enemy frequency or system that deprives friendly forces of that means of collecting data. Either interruption can significantly deter information collection efforts and their ability to answer critical information requirements. Coordination between the EWO, the fire support coordinator, and the G-2 (S-2) prevents this interference. In situations where a known conflict between the information collection effort and the use of EA exists, the CEMA working group brings the problem to the G-3 (S-3) for resolution.

Planners consider other effects that rely on electromagnetic spectrum when planning for EA. For example, military information support operations may include plans to use certain frequencies to broadcast messages, or a military deception plan may include the broadcast of friendly force communications. In both examples, the use of EA could unintentionally interfere or disrupt such broadcasts if not properly coordinated. To ensure EA does not negatively affect planned operations, the EWO coordinates between fires, network operations, and other functional or integrating cells as required.

Like any other form of electromagnetic radiation, EA can adversely affect local media and other communications systems and infrastructure. EW planners consider unintended consequences of EW operations and deconflict these operations with the various functional or integrating cells. For example, friendly jamming could potentially deny the functioning of essential services such as ambulance or firefighters to a local population. EWOs routinely synchronize EA with the other functional or integrating cells responsible for the information tasks. In this way, they ensure that EA efforts do not cause fratricide or unacceptable collateral damage to their intended effects.

The potential for hostile intelligence collection also affects EA. A well-equipped enemy can detect friendly EW activities and thus gain intelligence on friendly force intentions.

The effects of jamming only persist as long as the jammer itself is emitting and is in range to affect the target. Normally these effects last a matter of seconds or minutes, which makes the timing of such missions critical. This is particularly true when units use jamming in direct support of aviation 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 enemy air defensive countermeasures. Aside from antiradiation missiles, the effects of jamming are less persistent than effects achieved by other means.

A. GROUND-BASED Electronic Warfare Considerations

Ground-based EW capabilities support the commander's scheme of maneuver. Soldiers can use ground-based EW equipment when dismounted or on highly mobile platforms. Due to the short range nature of tactical signals direction finding, EA assets are normally located in the forward areas of the battlefield, with or near forward units.

Ground-based EW capabilities have certain advantages. They provide direct support to maneuver units (for example, through CREW and communications or sensor jamming). Soldiers use ground-based EW capabilities to support continuous operations and to respond quickly to EW requirements of the ground commander. However, to maximize the effectiveness of ground-based EW capabilities, maneuver units must protect EW assets from enemy ground and aviation threats. EW equipment should be as survivable and mobile as the force it supports. Maneuver units must logistically support the EW assets, and supported commanders must clearly identify EW requirements.

Ground-based EW capabilities have certain limitations. They are vulnerable to enemy attack and can be masked by terrain. They are vulnerable to enemy electromagnetic deceptive measures and EP activities. In addition, they have distance or propagation limitations against enemy electronic systems. As with any spectrum-based system, units must properly program EW equipment to avoid friendly interference and compatibility issues.

B. AIRBORNE Electronic Warfare Considerations

While ground-based and airborne EW planning and execution are similar, they significantly differ in their EW employment time. Airborne EW operations are conducted at much higher speeds and generally have a shorter duration than ground-based operations. Therefore, the timing of support from airborne EW assets requires detailed planning. Airborne EW requires the following:

- A clear understanding of the supported commander's EW objectives.
- Ground support facilities.
- Liaisons between the aircrews of the aircraft providing the EW effects and the aircrews or ground forces being supported.
- Protection from enemy aircraft and air defense systems.

Airborne EW capabilities have certain advantages. They can provide direct support to other tactical aviation missions such as suppression of enemy air defenses, destruction of enemy air defenses, and employment of high speed antiradiation missiles. They can provide extended range over ground-based assets. In addition, they can support ground-based units in beyond line-of-sight operations.

Limitations associated with airborne EW capabilities include limited time on station, vulnerability to enemy air defense systems, enemy EP actions, electromagnetic deception techniques, and limited assets.

See following pages (pp. 3-28 to 3-31) for discussion of Airborne Electronic Attack.

EMI Mitigation

EMI mitigation begins with operator-level troubleshooting and reporting. Troubleshooting may identify the source of the interference as truly EMI or an equipment or operator failure. Reporting facilitates situational understanding and supports the development of solutions. See table 3-1 below for steps to mitigate EMI problems.

EMI Troubleshooting Checklist

Step	*Tasks*
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 joint spectrum interference resolution report to S-6.
EMI S-6	electromagnetic interference signal staff officer

Ref: ATP 3-36(Dec '14), table 3-1. Operator EMI troubleshooting checklist.

E. Joint Spectrum Interference Resolution (JSIR)

All prohibitive EMI is reported and investigated through the joint spectrum interference resolution (JSIR) program. Some procedural guidance in support of the JSIR program may apply to command relationships such as military departments, Army commands, and combatant commands. The G-6 (S-6) and spectrum manager are also good sources of information.

CJCSI 3320.02F contains guidance for this program. CJCSM 3320.02D contains procedures for JSIR.

F. Joint Restricted Frequency List Deconfliction (JRFL)

The Army is transitioning away from the joint restricted frequency list (JRFL) and adopting spectrum management operations as the technique to deconflict EA from interference with friendly radio frequencies. One reason for this is that the JRFL does not adequately inform communications planners about EA frequencies in use. Therefore, EW planners must utilize the JRFL during mission planning and execution to mitigate the effects of offensive and defensive EA on friendly systems.

The JRFL is a concise list of highly critical frequencies that should not be jammed or attacked and is used by various operational, intelligence, and support elements. Critical frequencies may include various sensors, exploitation frequencies, full motion video feeds, networks of the mission command system, and aviation safety of flight frequencies. It includes command channels of senior commanders, but unfortunately does not include the frequencies used by maneuver Soldiers in contact with the enemy. The JRFL also does not provide protection from other spectrum users. That protection is provided by a valid frequency assignment coordinated through the G-6 (S-6) spectrum manager. JRFL entries are limited to the minimum number of radio frequencies and intelligence equities necessary for friendly forces to accomplish mission objectives.

Refer to FM 6-02.70 for more information about the JRFL.

The JRFL should not be mistaken as a fix for all deconfliction issues. High priority nets, bands, and frequencies are protected to a certain degree from friendly EA. However, spectrum managers must balance the competing demands that all friendly systems have the ability to operate unimpaired. This can be accomplished by simply adding the offending jammer to a database and using spectrum management techniques (such as changing frequencies, changing assignments, or moving to an unaffected area) to accomplish the mission.

I(a). Cyberspace (CEMA) Operations Planning

Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), chap. 3, app. B, and app C.

The commander and staff include the cyberspace planner during the MDMP for operations. The cyberspace planner is the subject matter expert to create effects in cyberspace and the EMS, with considerations from the CEMA section. Involving the cyberspace planner early in development of the commander's vision and planning allows for synchronization and integration with missions, functions, and tasks. A consideration of cyberspace operations is the lead time required for effects support. Early involvement, inclusion in operations orders preparation, and effects approval early in the process enhance the possibility of effects in cyberspace and the EMS supporting an operation. The two primary methodologies commanders and staffs use for planning cyberspace and EW operations are the Army design methodology and the MDMP.

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). Planning is one of the four major activities of mission command that occurs during operations process (plan, prepare, execute, and assess). Commanders apply the art of command and the science of control to ensure cyberspace and EW operations support the concept of operations.

The full scope of planning for cyberspace and EW operations is not addressed by the Army design methodology or the MDMP. These methodologies will allow Army forces to determine where and when effects in cyberspace and EW can be integrated to support the concept of operations. Army forces plan, prepare, execute, and assess cyberspace and EW operations in collaboration with the joint staff and other joint, interorganizational, and multinational partners as required. Whether cyberspace and EW operations are planned and directed from higher headquarters or requested from tactical units, timely staff actions and commander's involvement coupled with continued situational awareness of cyberspace and the EMS are critical for mission success.

Army commanders and staffs will likely coordinate or interact with joint forces to facilitate cyberspace operations. For this reason, commanders and staffs must have an awareness of joint planning systems and processes that facilitate cyberspace operations. Some of these processes and systems include the—

- Joint Planning Process *(see pp. 4-41 to 4-44)*
- Adaptive Planning and Execution System
- Review and Approval Process Cyberspace Operations *(refer to CJCS Manual 3139.01 and appendixes A and C).*

Refer to BSS5: The Battle Staff SMARTbook, 5th Ed. for further discussion. BSS5 covers the operations process (ADRP 5-0); commander's activities (Understand, Visualize, Describe, Direct, Lead, Assess); the military decisionmaking process and troop leading procedures (FM 6-0: MDMP/TLP); integrating processes and continuing activities (IPB, targeting, risk management); plans and orders (WARNOs/FRAGOs/OPORDs); mission command, command posts, liaison; rehearsals & after action reviews; and operational terms & symbols.

I. Army Design Methodology (Including Cyberspace and Electronic Warfare Operations)

The Army design methodology is a methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them. Given the unique and complex nature of cyberspace, commanders and staffs benefit from implementing the Army design methodology to guide more detailed planning during the MDMP.

Framing an operational environment involves critical and creative thinking by a group to build models that represent the current conditions of the operational environment (current state) and models that represent what the operational environment should resemble at the conclusion of an operation (desired end state). A planning team designated by the commander will define, analyze, and synthesize characteristics of the operational and mission variables and develop desired future end states. Cyberspace should be considered within this framing effort for opportunities as they envision desired end states.

Framing a problem involves understanding and isolating the root causes of conflict discussed and depicted in the operational environment frame. Actors may represent obstacles for commanders as they seek to achieve desired end states. Creating and employing cyberspace capabilities shapes conditions in the operational environment supporting the commander's objectives.

II. The Military Decision-Making Process (with Cyberspace and Electronic Warfare Operations)

Cyberspace and EW operations planning is integrated into MDMP, an iterative planning methodology to understand the situation and mission, develop a course of action (COA), and produce an operation plan or order (ADP 5-0). The commander and staff integrate cyberspace and EW operations throughout the MDMP. They ensure courses of action are supported by the scheme of cyberspace operations and meet requirements for suitability, feasibility, and acceptability. Staff members responsible for planning and integrating cyberspace operations participate in the MDMP events and CEMA working groups. The MDMP consists of the following seven steps—

Step 1: Receipt of Mission

Commanders initiate the MDMP upon receipt or in anticipation of a mission. Staff members responsible for planning and integrating cyberspace and EW operations initiate coordination with higher headquarters staff counterparts to obtain information on current and future cyberspace and EW operations, running estimates, and other cyberspace and EW operations planning products.

MDMP Step 1: Receipt of Mission

Key Inputs	Process	Key Outputs
Higher headquarters plan or order Planning products from higher headquarters including the cyberspace effects running estimate	Begin updating the cyberspace effects and electronic warfare running estimates Gather the tools to prepare for mission analysis specific to cyberspace operations Provide cyberspace and electronic warfare operations input for formulation of the commander's initial guidance and the initial warning order	Updated cyberspace effects and electronic warfare running estimate

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

Operational (PMESII-PT) & Mission Variables (METT-TC)

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. 2-20 to 2-21 for related discussion of operational and mission variables as related to cyberspace operations.

Step 2: Mission Analysis

Commanders and staffs perform mission analysis to better understand the situation and problem, identify what the command must accomplish, when and where it must be done, and why (the purpose of the operation). Staff members responsible for planning and integrating cyberspace and EW operations gather, analyze, and synthesize information on current conditions of the operational environment with an emphasis on cyberspace, the EMS, and the information environment.

MDMP Step 2: Mission Analysis

Key Inputs	Process	Key Outputs
Commander's initial guidance	Analyze inputs and develop information requirements	List of cyberspace information requirements
Army design methodology product	Participate in the intelligence preparation of the battlefield process	Intelligence preparation of the battlefield products to support cyberspace and electronic warfare operations
Higher headquarters' plans, orders, or knowledge products	Identify and develop high-value targets	Most likely and most dangerous enemy courses of action
	Identify vulnerabilities of friendly, enemy, adversary, and neutral actors	List of cyberspace operations specific and implied tasks
	Determine cyberspace and electronic warfare operations specified, implied, and essential tasks	List of cyberspace limitations and constraints
	Determine cyberspace operations limitations and constraints	List of cyberspace assumptions
	Identify cyberspace critical facts and assumptions	Updated cyberspace operations running estimate
	Identify and nominate cyberspace related commander's critical information requirements	
	Identify and nominate cyberspace critical information	
	Provide input to the combined information overlay	
	Provide input for the development of the mission analysis brief and warning order	
	Participate in the mission analysis brief	

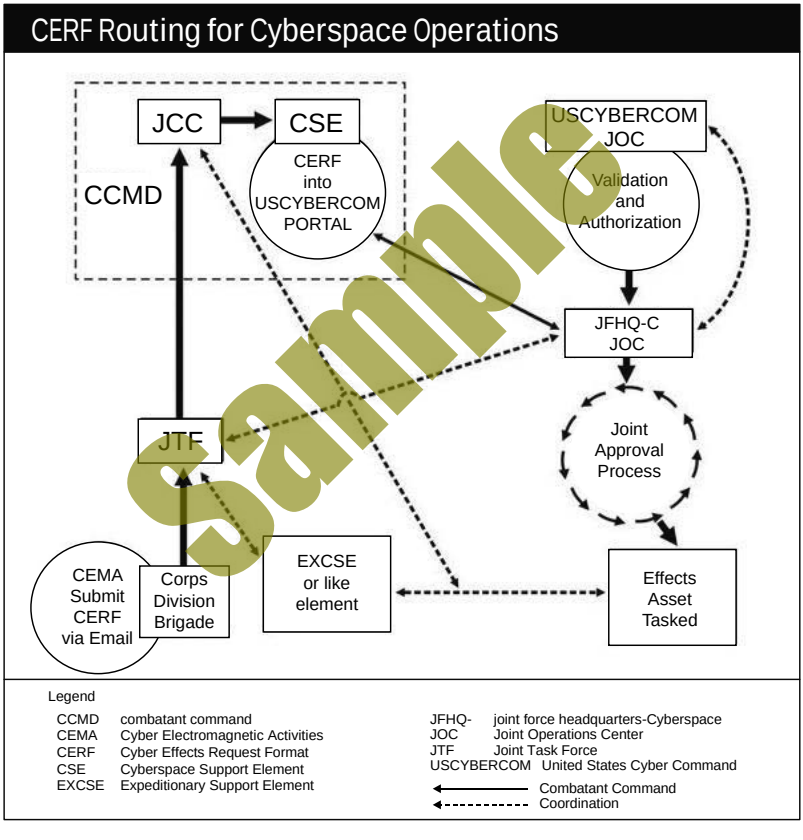
Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), table 3-3.

I(b). Cyber Effects Request Format (CERF)

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

I. Requesting Cyberspace Effects

The CERF is the format forces use to request effects in and through cyberspace. Effects in cyberspace can support operations in any domain. Execution orders provide authorization to execute cyberspace effects. Support in response to CERFs may be from joint cyberspace forces such as the combat mission teams, from other joint or service capabilities, or from service retained cyberspace forces.



FM 3-12, fig. C-1. Cyber effects request format routing for cyberspace operations.

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 approves and processes the CERF. This happens at each echelon until the CERF reaches a joint headquarters

II. Joint Electronic Warfare Planning Process

Ref: JP 3-13.1, Electronic Warfare (Feb '12), pp. III-6 to II-12.

In order to be fully integrated into other aspects of a planned operation, the EWC conducts joint EW planning beginning as early as possible and coordinates it with other aspects of the plan throughout the joint operation planning process (JOPP). Figure III-2 shows the integration of EW into the JOPP. Thorough EW planning will minimize EMS conflicts and enhance EW effectiveness during execution. Proper EW planning requires understanding of the joint planning and decision-making processes; nature of time-constrained operations; potential contributions of EW; and employment of joint EW. During execution, EW planners must monitor the plan's progress and be prepared to make modifications to the plan as the dynamics of the operation evolve. Joint EW planners should take the following actions during the planning process to integrate EW into the joint plan:

- Determine the type, expected length, geographic location, and level of hostility expected during the operation to be planned.
- Review the scale of anticipated operations and the number and type of friendly forces (to include allied and coalition partners) expected to participate.
- Review current ROE and existing authorities for EW activities and recommend any necessary modifications in accordance with current staff procedures. Coordinate with the staff judge advocate to ensure requirements of ROE, legal authorities, and LOAC are met.
- Review, with the NETOPS community, the contribution EW can make to protect the EMS for use by the DOD information networks. This should be done through the J-6 representative assigned to the JCEWS or EWC staff.
- Review, with other planners, the contribution EW can make to efforts in other mission areas (e.g., military information support operations [MISO], MILDEC, and CNO) and determine the level of EW platform support they expect to need during the operation.
- Review the role EW capabilities can play in creating NAVWAR effects and determine the level of EW platform support they expect to need during the operation.
- Review, with intelligence planners, the type of ES platforms, capabilities, and products available to support the operation. IGL analysis of EW actions should start early and be frequently reviewed during the planning and execution phases of an operation.
- Consult with Service, functional component, and multinational EW planners, wherever the most current and relevant expertise in the employment of EW capabilities resides, in order to understand and remain current on the full range of EW capabilities available for accomplishing operational objectives.
- Work in concert with J-6 EMS managers to improve awareness and deconflict all military, civilian, and other systems (e.g., communication systems, sensors, and EMS-dependent weapon systems) that could impact the EMOE.
- Determine the number and type of EW platforms that could reasonably be expected to be tasked to support the joint operation being planned. Consult automated force status reports (e.g., those provided through the Defense Readiness Reporting System for US forces) for this information. Service and functional components and multinational planners should be consulted to augment automated information.
- Review, with component air planners, the requirement for EW support to the SEAD effort.
- Recommend, to the EWC director (or other designated member of the J-3 or J-5 staff), the type and number of EW assets to be requested from component or supporting commands for the operation being planned.
- Estimate the size and expertise of the EW staff required to plan and coordinate execution of the EW portion of the plan. Consult with Service, functional component, and multinational EW planners to refine these estimates.

- Recommend how best to effectively prosecute EW operations to create NAVWAR effects and maintain a PNT advantage. Estimate the impact of NAVWAR effects on both military objectives and civil/commercial users.
- Recommend staff augmentation in accordance with staff procedures from component, supporting, and multinational forces (MNFs) as necessary to assemble the staff required to conduct EW planning.
- Coordinate with the combatant command JFMO or JSME early in the planning process to determine if JSC assistance is required.
- During crisis action planning, evaluate each COA considered with respect to EW resources required and the EW opportunities and vulnerabilities inherent in the COA.
- Integrate EW into joint targeting.

EWC Actions and Outcomes as Part of Joint Planning

Planning Process Steps	Electronic Warfare (EW) Cell Planning Action	EW Cell Planning Outcome
Planning Initiation	• Monitor situation. • Review guidance and estimates. • Convene EW cell. • Ensure EW representation within information operations (IO) cell. • Gauge initial scope of the EW role. • Identify organizational coordination requirements. • Initiate identification of information required for mission analysis and course of action (COA) development. • Validate, initiate, and revise priority intelligence requirements (PIRs) and requests for information (RFIs). • Recommend EW strategies and conflict resolution.	Request taskings to collect required information.
Mission Analysis	• Identify specified, implied, and essential EW tasks. • Identify assumptions, constraints, and restraints relevant to EW. • Identify EW planning support requirements (including augmentation) and issue requests for support. • Initiate development of measures of effectiveness and measures of performance. • Analyze EW capabilities available and identify authority for deployment and employment. • Obtain relevant physical, informational, and cognitive properties of the information environment from the IO cell. • Refine proposed PIRs/RFIs. • Provide EW perspective in the development of restated mission for commander's approval. • Tailor augmentation requests to missions and tasks.	List of EW tasks. List of assumptions, constraints, and restraints. Planning guidance for EW. EW augmentation request. EW portion of the commander's restated mission statement.
COA Development	• Select EW supporting and related capabilities to accomplish EW tasks for each COA. • Revise EW portion of COA to develop staff estimate. • Provide results of risk analysis for each COA.	List of objectives to effects to EW tasks to EW capabilities for each COA.
COA Analysis and Wargaming	• Analyze each COA from an EW functional perspective. • Identify key EW decision points. • Recommend EW task organization adjustments. • Provide EW data for synchronization matrix. • Identify EW portions of branches and sequels. • Identify possible high-value targets related to EW. • Recommend EW commander's critical information requirements.	EW data for overall synchronization matrix. EW portion of branches and sequels. List of high-value targets related to EW.
COA Comparison	• Compare each COA based on mission and EW tasks. • Compare each COA in relation to EW requirements versus available EW resources. • Prioritize COAs from an EW perspective.	Prioritized COAs from an EW perspective with pros and cons for each COA.
COA Approval	• No significant EW staff actions during COA approval.	Not applicable.
Plan or Order	• Refine EW tasks from the approved COA. • Identify EW capability shortfalls and recommended solutions. • Update continually all supporting organizations regarding details of the EW portion of plan details (access permitting). • Advise supported combatant commander on EW issues and concerns during supporting plan review and approval. • Participate in time-phased force and deployment data (TPFDD) refinement to ensure the EW force flow supports the concept of operations.	Updated EW estimates based on selected COA. Draft EW appendices and tabs, supporting plans. EW requirements to TPFDD development. Synchronized and integrated EW portion of operation plan.

JP 3-13.1, fig. III-2. Electronic Warfare Cell Actions and Outcomes as Part of Joint Planning.

II(b). Electronic Attack Request Format (EARF)

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

I. Electronic Attack Request Format (EARF)

Request EA effects via normal request processes and provide specific effects requests using the EARF. The EARF normally accompanies the joint tactical air strike request.

For more information on this format refer to ATP 3-09.32.

Format 24. Electronic Attack Request Format (EARF)	
Requesting Major Supported Command:	
Requesting Unit:	
Contact Information: This person will be responsible to verify that the EARF has been approved before the mission starts and to relay the information to the executing unit.	
Joint Tactical Air Request (JTAR) Number: Enter the corresponding JTAR number that will be submitted with this EARF.	
Concept of Operations: Describe the concept of operations. This will include the objective, forces used, timeline of the mission, and coordination efforts required for mission success. Relate the impact of mission success to specific objectives for the integrated tasking order.	
Electronic Attack (EA) Concept of Operations: Define desired effect(s) and timeline.	
Cease Buzzer Procedures: This will be in accordance with theatre special instructions (SPINS). Provide frequency to communicate between jamming control authority (JCA) and EA asset. Very/ultra-high frequency (V/UHF) is the primary means to talk to a supporting aircraft. If unable to establish communications, consider using another asset to relay information. Some aircraft may be Internet Relay Chat (IRC) client (mIRC) capable.	
Friendly Frequency Use for Operation:	
Target Communications System(s) to be Jammed/Denied:	Target Requested (List type and frequency, if known.) Intelligence Assessment (Intelligence assessment required for each request. Do not copy and paste frequencies from one day to the next without intelligence validation/assessment.)
Target Location (in Lat/Long or military grid reference system [MGRS]):	
Jamming date-time group(s): From – To, in Zulu Time (preferred)	
Type of EA Requested: Preplanned – Scheduled/On-Call	

Ref: FM 3-12, table D-1. The electronic attack request format.

II. Electronic Attack 5 Line

Request immediate and on-call EA requests using a 5-line format. This is used to prepare the aircrew for an EA. For more information on this format see ATP 3-09.32.

See following page for an example of the EA 5-line briefing format.

III. Cyberspace (CEMA) Operations Targeting

Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), pp. 3-21 to 3-25 and Ref: ATP 3-36, Electronic Warfare Techniques (Dec '14), chap. 4.

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 is an integrating and iterative process that occurs throughout the major activities of the operations process. The functions of decide, detect, deliver, and assess define the targeting process and occur simultaneously and sequentially during the operations process. Targeting activities for cyberspace and EW operations which involve the employment of cyberspace and EW effects closely follow standard targeting processes.

Targets identified through the operations process appear on the integrated target list. Organic cyberspace and EW capabilities, with the proper authority, may fulfill the desired effect on the target. Time and synchronization issues may affect the decision to use organic assets as well as the legal and operational authorities. The capability to affect targets may require proximity of capabilities and operational reach access.

If the unit's organic capabilities or authorities do not fulfill the targeting requirements to support the commander's intent, they request support from the next higher echelon. As requests pass from echelon to echelon, each unit processes the target packet or request to use organic capabilities and authorities to support the subordinate unit's requirement. The requirement elevates until it reaches an echelon that can support the requirement with the appropriate capabilities and authority, or the request for targeting is denied. Fulfilling cyberspace and EW effects requests on targets may not be possible due to prioritization, timing, capabilities, authorization, or conflict with other cyberspace and EW capability requirements.

Identifying targets early in the planning process is key to approval and synchronization. Integrating the targets into the normal targeting process identifies if the organic capabilities can achieve the desired effects. Due to their impact, some cyberspace and EW effects delivery capabilities (such as EA) require synchronization and coordination across the entire staff. Some effects may prohibit friendly use of cyberspace and EW, knowingly or inadvertently, and the situational awareness of the cyberspace and EW operation will enable the staff in taking the appropriate remediation actions and decisions.

OCO and EW targets not available for effects through Army means may continue to joint echelons for processing. The targets may require additional joint force cyberspace or EW assets to support the Army commander mission. This could result in the corps and below targets being included on the joint integrated prioritized target list. In addition, targets developed with the initial intention to employ cyberspace and EW effects may be struck with lethal fires or engaged through other non-lethal means.

See pp. 1-46 to 1-48 for related discussion of targeting in and through cyberspace from JP 3-12.

Refer to BSS5: The Battle Staff SMARTbook, 5th Ed. for further discussion. BSS5 covers the operations process (ADRP 5-0); commander's activities (Understand, Visualize, Describe, Direct, Lead, Assess); the military decisionmaking process and troop leading procedures (FM 6-0: MDMP/TLP); integrating processes and continuing activities (IPB, targeting, risk management); plans and orders (WARNOs/FRAGOs/OPORDs); mission command, command posts, liaison; rehearsals & after action reviews; and operational terms & symbols.

Electronic Warfare (EW) Targeting

Ref: ATP 3-36, Electronic Warfare Techniques (Dec '14), pp. 4-1 to 4-2.

The modern battlefield presents more targets than available resources can acquire and attack. The commander determines which targets are the most important to the enemy and which ones must be acquired and attacked. As the operation continues, the staff assesses the results.

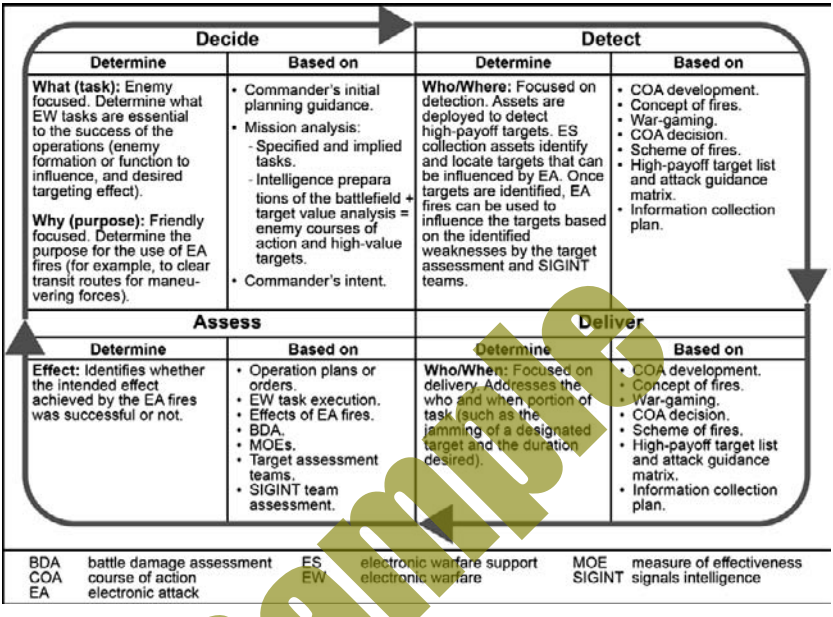


Figure 4-1. Electronic warfare in the targeting process

Ref: ATP 3-36 (Dec '14), fig. 4-1. Electronic warfare in the targeting process.

The EWO thoroughly integrates EA in the targeting process and integrates EA fires into all appropriate portions of the operation plan, operation order, and other planning products. To support EW targeting, the EWO—

- Helps the targeting working group determine EA requirements against specific high-payoff targets and high-value targets.
- Ensures EA can meet the desired effect (in terms of the targeting objective).
- Ensures EA will not adversely affect friendly electromagnetic spectrum use.
- Coordinates with the SIGINT staff element through the collection manager to satisfy ES and EA information requirements.
- Provides EA mission management through the command post or joint operations center and the tactical air control party (for airborne electronic attack).
- Provides EA mission management as the electronic warfare control authority for ground or airborne electronic attack when designated.
- Determines and requests theater Army EA support.
- Recommends to the G-3 (S-3) and the fire support coordinator or fire support officer whether to engage a target with EA.
- Expedites EMI reports to the targeting working group.

Appendix 12 to Annex C (Sample Format)

Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), app B.

[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*

Continued on next page

Continued on next page

[page number]
[CLASSIFICATION]

V. Cyberspace Integration into Joint Planning (JPP)

Ref: U.S. Army War College Strategic Cyberspace Operations Guide (Jun '16), chap. 3 and JP 5-0, Joint Planning (Jun '17), chap. V.

Joint planning is the deliberate process of determining how (the ways) to use military capabilities (the means) in time and space to achieve objectives (the ends) while considering the associated risks.

Joint Planning Process (JPP)

The joint planning process (JPP) is an orderly, analytical set of logical steps to frame a problem; examine a mission; develop, analyze, and compare alternative COAs; select the best COpA; and produce a plan or order. JPP helps commanders and their staffs organize their planning activities, share a common understanding of the mission and commander's intent, and develop effective plans and orders.

Joint Planning Process (JPP) Steps

I **Planning Initiation**

II **Mission Analysis**

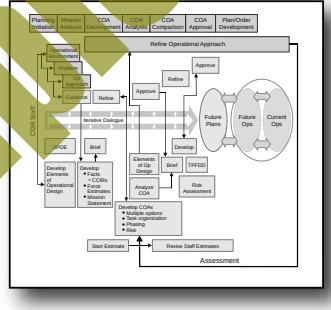
III **COA Development**

IV **COA Analysis and Wargaming**

V **COA Comparison**

VI **COA Approval**

VII **Plan or Order Development**



Ref: JFODS5: The Joint Forces Operations & Doctrine SMARTbook and JP 5-0.

Refer to JFODS5: The Joint Forces Operations & Doctrine SMARTbook (Guide to Joint, Multinational & Interorganizational Operations) for further discussion. Topics and chapters include joint doctrine fundamentals (JP 1), joint operations (JP 3-0), joint planning (JP 5-0), joint logistics (JP 4-0), joint task forces (JP 3-33), information operations (JP 3-13), multinational operations (JP 3-16), interorganizational cooperation (JP 3-08), plus more!

VI. Integrating / Coordinating Functions of IO

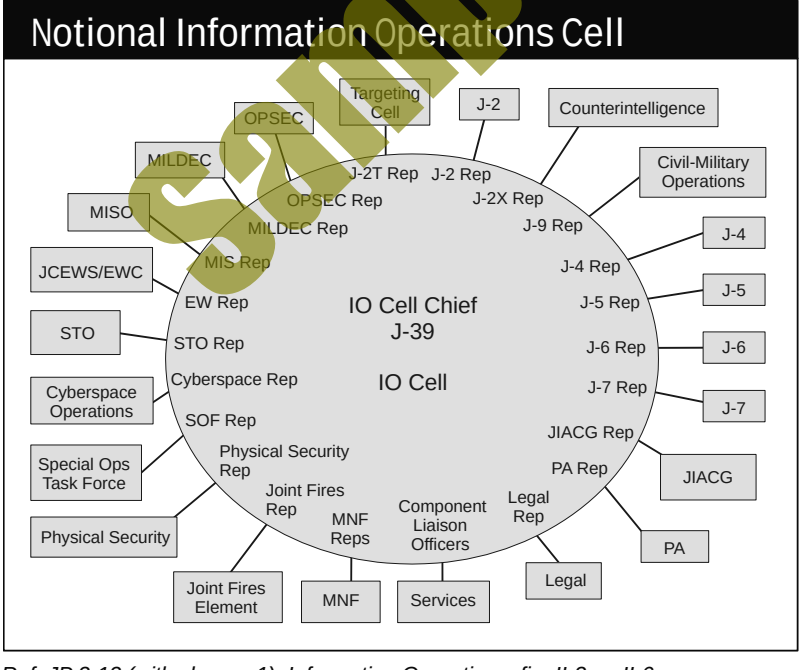
Ref: JP 3-13 w/change 1, Information Operations (Nov '14), chap. II.

This section addresses how the integrating and coordinating functions of IO help achieve a JFC's objectives. Through the integrated application of IRCs, the relationships that exist between IO and the various IRCs should be understood in order to achieve an objective.

See pp. 0-10 to 0-15 for related discussion of the information environment, information as a joint function, and information operations (IO).

I. Information Operations and the Information-Influence Relational Framework

Influence is at the heart of diplomacy and military operations, with integration of IRCs providing a powerful means for influence. The relational framework describes the application, integration, and synchronization of IRCs to influence, disrupt, corrupt, or usurp the decision making of TAs to create a desired effect to support achievement of an objective. Using this description, the following example illustrates how IRCs can be employed to create a specific effect against an adversary or potential adversary.



Ref: JP 3-13 (with change 1), Information Operations, fig. II-3, p. II-6.

II. The Information Operations Staff and Information Operations Cell

Within the joint community, the integration of IRCs to achieve the commander's objectives is managed through an IO staff or IO cell. JFCs may establish an IO staff to provide command-level oversight and collaborate with all staff directorates and supporting organizations on all aspects of IO. Most CCMDs include an IO staff to serve as the focal point for IO. Faced with an ongoing or emerging crisis within a geographic combatant commander's (GCC's) area of responsibility (AOR), a JFC can establish an IO cell to provide additional expertise and coordination across the staff and interagency.

IO Staff

In order to provide planning support, the IO staff includes IO planners and a complement of IRCs specialists to facilitate seamless integration of IRCs to support the JFC's concept of operations (CONOPS). IRC specialists can include, but are not limited to, personnel from the EW, cyberspace operations (CO), military information support operations (MISO), civil-military operations (CMO), military deception (MILDEC), intelligence, and public affairs (PA) communities. They provide valuable linkage between the planners within an IO staff and those communities that provide IRCs to facilitate seamless integration with the JFC's objectives.

IO Cell

The IO cell integrates and synchronizes IRCs, to achieve national or combatant commander (CCDR) level objectives. Normally, the chief of the CCMD's IO staff will serve as the IO cell chief; however, at the joint task force level, someone else may serve as the IO cell chief. The IO cell comprises representatives from a wide variety of organizations to coordinate and integrate additional activities in support of a JFC. It may include representatives from organizations outside DOD, even allied or multinational partners.

III. Relationships and Integration

IO is not about ownership of individual capabilities but rather the use of those capabilities as force multipliers to create a desired effect. There are many military capabilities that contribute to IO and should be taken into consideration during the planning process.

Commander's Communications Synchronization (CCS)

Commander's Communication Synchronization (CCS) entails focused efforts to create, strengthen, or preserve conditions favorable for the advancement of national interests, policies, and objectives by understanding and communicating with key audiences through the use of coordinated information, themes, messages, plans, programs, products and actions, synchronized with the other instruments of national power.

Refer to Joint Doctrine Note 2-13, CCS (Dec '13) for more information.

A. Strategic Communication (SC)

The SC process consists of focused United States Government (USG) efforts to create, strengthen, or preserve conditions favorable for the advancement of national interests, policies, and objectives by understanding and engaging key audiences through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. SC is a whole-of-government approach, driven by interagency processes and integration that are focused upon effectively communicating national strategy.

Chap 5

I. Spectrum Management Operations (SMO/JEMSO)

Ref: JP 6-01, Joint Electromagnetic Spectrum Management Operations (Mar '12), chap. 1, FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), chap. 2; and ATP 6-02.70, Techniques for Spectrum Management Operations (Dec '15).

I. The Electromagnetic Spectrum (EMS)

The electromagnetic spectrum is the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (JP 3-13.1). The EMS is a physics-based maneuver space essential to control the operational environment during all military operations. The EMS is a highly regulated and saturated natural resource. The EMS includes the full range of all possible frequencies of electromagnetic (EM) radiation.

Military operations are complicated by increasingly complex demands on the electromagnetic spectrum (EMS). All modern forces depend on the EMS. The EMS is a physical medium through which joint forces conduct operations. EMS-dependent devices are used by both civilian and military organizations and individuals for intelligence; communications; position, navigation, and timing; sensing; command and control (C2); attack; ranging; chemical, biological, radiological, and nuclear (CBRN) sensor data collection/transmission; unmanned aircraft systems (UASs); civil infrastructure; data transmission and information storage and processing. The importance of the EMS and its relationship to the operational capabilities is the key focus of joint electromagnetic spectrum management operations (JEMSMO). JEMSMO is a functional area ultimately responsible for coordinating EMS access among multinational partners, throughout the operational environment.

See following pages (pp. 5-2 to 5-3) for further discussion of the EMS.

Spectrum Management Operations (Army)

The Army manages its use of the EMS through spectrum management operations (SMO). Spectrum management operations 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 (FM 6-02).

Electromagnetic spectrum operations (EMSO) include spectrum management operations (SMO) and electronic warfare (EW). SMO are the management functions of EMSO managing the man-made access to the EMS.

See p. 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.

Joint Electromagnetic Spectrum Operations (JEMSO)

JEMSO include all activities in military operations to successfully plan and execute joint or multinational operations in order to control the electromagnetic operational environment (EMOE). JEMSO is comprised of EW and JEMSMO and aims to exploit, attack, protect, and manage resources within the (EMOE) and resolve EMI in order to achieve the commander's objectives. Inherent within JEMSMO is spectrum management (SM).

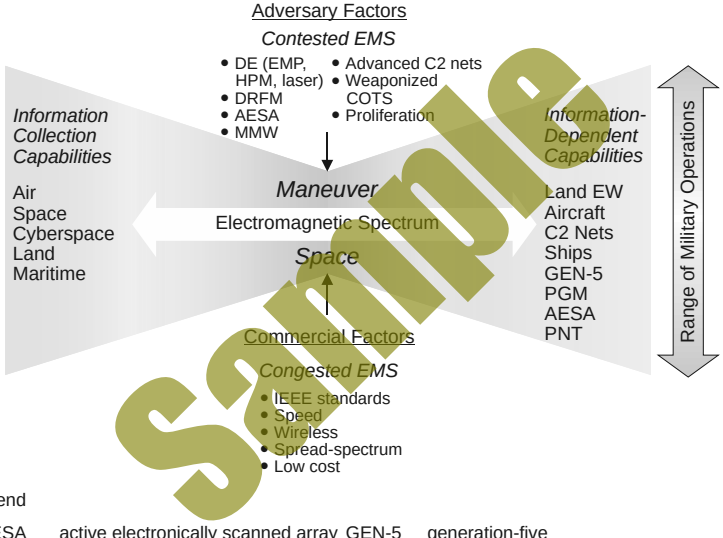
See pp. 5-4 to 5-5 for a discussion of the EMOE. See pp. 5-5 to 5-6 for further discussion of JEMSO.

A. The Electromagnetic Spectrum (EMS)

Ref: JP 6-01, Joint Electromagnetic Spectrum Management Operations (Mar '12), pp. I-1 to I-3.

The electromagnetic spectrum (EMS) is a physics-based maneuver space essential to control the operational environment during all military operations. Information and data exchange between platforms and capabilities will at some point rely on the EMS for transport. This maneuver space is constrained by both military and civil uses as well as adversary attempts to deny the use of the EMS, creating a congested and contested environment. This constrains freedom of maneuver to use all capabilities of friendly forces throughout the operational environment.

EMS Constraints on Military Operations



Legend

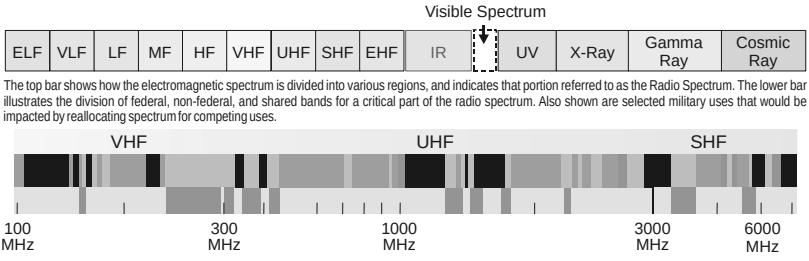
AESA	active electronically scanned array	GEN-5	generation-five
C2	command and control	HPM	high-power microwave
COTS	commercial off-the-shelf	IEEE	Institute of Electrical and Electronics Engineers
DE	directed energy		
DRFM	digital radio frequency memory	MMW	millimeter wave
EMP	electromagnetic pulse	PGM	precision-guided munition
EMS	electromagnetic spectrum	PNT	positioning, navigation, and timing
EW	electronic warfare		

Ref: JP 6-01, Joint Electromagnetic Spectrum Management Operations (Mar '12), fig. I-1. Electromagnetic Spectrum Constraints on Military Operations.

The EMS is a highly regulated and saturated natural resource. The EMS (Figure I-2) includes the full range of all possible frequencies of electromagnetic (EM) radiation. Frequency refers to the number of occurrences of a periodic event over time. For radio frequencies (RFs), this is expressed in cycles per second or hertz (Hz). Generally, the frequencies between 30 Hz and 300 gigahertz are referred to as the RF spectrum.

See fig. I-2, facing page.

The Electromagnetic Spectrum



The top bar shows how the electromagnetic spectrum is divided into various regions, and indicates that portion referred to as the Radio Spectrum. The lower bar illustrates the division of federal, non-federal, and shared bands for a critical part of the radio spectrum. Also shown are selected military uses that would be impacted by reallocating spectrum for competing uses.

Below 6 GHz:

Non-Federal Controlled Spectrum | Federal Controlled Spectrum | Shared Spectrum | Bands That Support DOD Capabilties

Bands That Support DOD Capabilities

(These bands are allocated within the US only. Spectrum allocation outside the US may be different.)

138 - 144 MHz

Military uses
Land mobile radio
Tactical air/ground/air

Competing uses
Little LEOs
Public safety

225 - 400 MHz

Military uses
Tactical air/ground/air
Data links
Satellite communications
Military ATC
Search and rescue
Executive communications

Tactical communications
Competing uses
Little LEOs
Public safety
Terrestrial DAB
CMRS
Space research

400.15 - 401 MHz

Military uses
DMSP (downlink)

Competing uses
MSS

420 - 450 MHz

Military uses
Ballistic missile surveillance and early warning radars
Missile/air vehicle flight Termination

Troop position location
Anti-stealth radar
Foliage penetration radar

1215 - 1390 MHz

Military uses
Long/medium range air defense
Radio navigation
Air route surveillance radars
Tactical communications
Test range support
Air/fleet defense
Drug interdiction

Global positioning system – satellite
Remote satellite sensors
Nuclear detection
Competing uses
MSS
NLMCS
Wind profiler
RADARs

1435 - 1525 MHz

Military uses
Telemetry supporting entire aerospace industry

Competing uses
DAB/DARS
MSS
NLMCS

1755 - 1850 MHz

Military uses
DOD satellite TT&C (uplink)
Point-to-point microwave
Air combat training systems
Tactical communications
Tactical data links

Competing uses
PCS
MDS
3G wireless/IMT 2000

2200 - 2290 MHz

Military uses
DOD satellite TT&C (downlink)
Guided missile telemetry
Point-to-point microwave

Competing uses
PCS
MDS
WLL

3100 - 3650 MHz

Military uses
High power mobile radars
Shipboard ATC
Missile links
Airborne station keeping

Competing uses
MDS
WLL
FSS

4400 - 4950 MHz

Military uses
Fixed wideband communications
Mobile wideband communications
Command links
Data links

Competing uses
GWCS
FSS
Public safety

Legend

ATC	air traffic control
CMRS	commercial mobile radio service
DAB	digital audio broadcast – terrestrial
DARS	digital audio radio service – satellite
DOD	Department of Defense
DMSP	Defense Meteorological Satellite Program
EHF	extremely high frequency
ELF	extremely low frequency
FSS	fixed satellite service
GHz	gigahertz
GWCS	general wireless communications service
HF	high frequency
IMT 2000	third generation mobile telephony
IR	infrared
LEO	low earth orbit
LF	low frequency
MDS	multipoint distribution system
MF	medium frequency
MHz	megahertz
MSS	mobile satellite service
NLMCS	new land mobile communications service
PCS	personal communications service
SHF	super-high frequency
TT&C	telemetry, tracking, and commanding
UHF	ultrahigh frequency
UV	ultraviolet
VHF	very high frequency
VLF	very low frequency
WLL	wireless local loop

While JP 6-01 focuses primarily on the RF portion of the EMS, it should be noted that emergent technologies, capabilities, and systems (e.g., free space optics, infrared and laser technologies, and electronic warfare [EW] devices) are under development and being fielded that operate across the RF and non-RF portions of the EMS and must be considered. As the RF portion of the spectrum becomes more saturated, it can be expected that the use of higher frequencies will be developed to support communications, intelligence, and weapons systems and capabilities, and require planning and management.

Allied EMS Management Authorities

Ref: JP 6-01, Joint Electromagnetic Spectrum Management Operations (Mar '12), pp. II-1 to II-4.

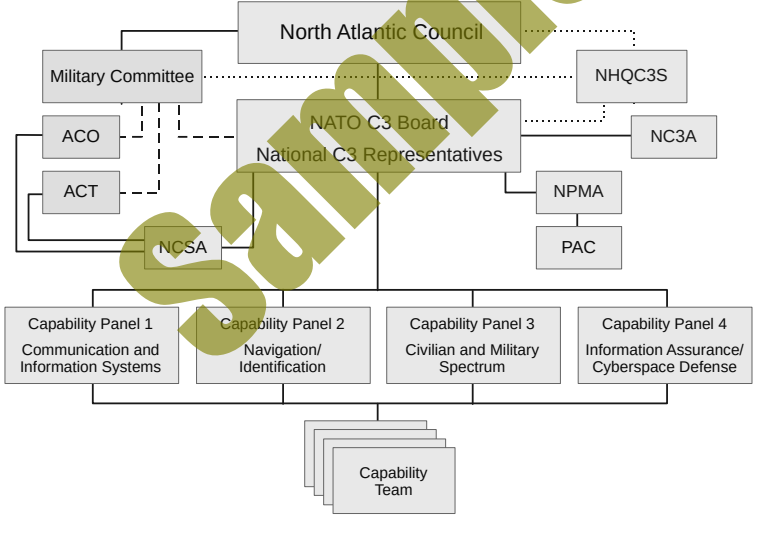
A. North Atlantic Treaty Organization (NATO)

NATO is a political and military alliance of 26 European and two North American nations. NATO organizations that have a role in EMS management operations are:

Military Committee (MC) is the senior military authority in NATO, providing NATO's civilian decision-making bodies—the North Atlantic Council, the Defense Planning Committee, and the Nuclear Planning Group—with advice on military matters.

The **Civilian/Military Spectrum Capability Panel** works directly for the MC on consultation, command, and control issues and is the sole competent source of advice and decisions on the management of the RF spectrum within NATO (see Figure II-1). It supports the MC and works with the strategic commands to satisfy NATO RF spectrum requirements during peace, emergency, crisis, and wartime. The NATO Civilian/Military Spectrum Capability Panel is also responsible for maintaining the NATO supplements to Allied Communications Publication (ACP) 190, Guide to Spectrum Management in Military Operations.

NATO Spectrum Management Authorities



Legend

ACO	Allied Command Operations (SHAPE)	NPMA	NATO PKI Management Agency
ACT	Allied Command Transformation (Norfolk, VA)	PAC	PKI Advisory Cell
C3	command, control, and communications	PKI	public key infrastructure
NATO	North Atlantic Treaty Organization	SHAPE	Supreme Headquarters Allied Powers Europe
NC3A	NATO Consultation, Command, and Control (C3) Agency	———	command and control
NCSA	NATO Communication and Information Systems Services Agency	·····	communications
NHQC3S	NATO Headquarters C3 Staff	- - - -	coordination

Ref: JP 6-01 (Mar '12), fig. II-1. NATO Spectrum Management Authorities.

The **Civilian/Military Spectrum Capability Panel** is composed of representatives from the military and civil SM components of NATO member nations; the strategic commands; and the NATO Consultation, Command, and Control Agency (an acquisition and development organization). The Civilian/Military Spectrum Capability Panel also interacts with non-NATO nations in support of cooperative efforts involving frequency and SM issues. It may also deal with the military frequency and spectrum problems of other agencies/organizations, any separate NATO command that may be established later, or of the NATO nations (when called upon), provided this does not interfere with its primary mission.

The **NATO Headquarters Consultation, Command, and Control Staff Spectrum Management Branch (SMB)** is the day-to-day staff charged with carrying out the necessary staff and operational work in support of the Civilian/Military Spectrum Capability Panel and the NATO nations and commands. Staff work includes diverse activities such as developing spectrum vision for NATO; developing and maintaining NATO spectrum policy and doctrine; providing advice to nations, organizations, and acquisition programs for spectrum-dependent equipment involving frequencies and spectrum; coordinating supportability assessments; management of the NATO portions of the 225–400 MHz band; and other tasks in support of the Civilian/Military Spectrum Capability Panel terms of reference (see the FM Handbook for more information).

National Radio Frequency Agency. The SM office for the ministry of defense or chief of defense that acts as the national military frequency agency for a nation is usually called a national RF agency. This agency exists as the single interface for frequency and spectrum coordination and management issues between the Civilian/Military Spectrum Capability Panel SMB and the NATO nation on a national military level. See ACP 190(C), Guide to Spectrum Management in Military Operations, ACP190, NATO Supplement (SUPP)-1B, NATO Guide to Spectrum Management in Military Operations, NATO Frequency Management Handbook, and CCEB Publication 1, Organization, Roles, Policies, and Responsibilities for more information on Allied SM organizations.

B. The Combined Communications–Electronics Board (CCEB)

The CCEB is a five-nation, joint military communications–electronics (C-E) organization whose mission is the coordination of any military C-E matter that is referred to it by a member nation.

The member nations of the CCEB are Australia, Canada, New Zealand, the United Kingdom, and the US.

The CCEB has no standing forces so their focus is on interoperability between member nations. The CCEB principals consist of a senior communications representative from each of the member nations.

The **spectrum working group (WG)** is the CCEB WG concerned with CCEB SM issues.

Historically, CCEB nations have had a major positive impact on NATO's wider allied communications (technical) interoperability through the generation and distribution of communications procedural documents titled ACPs. ACPs are issued as guidance for, and use by, allied forces of the nations represented on the CCEB and are appropriate for use in any theater or part of the world. The ACP base publications do not contain national or local theater, command, or geographically significant information. ACP supplements are provided to cover specific national, command, or geographic issues. Two key ACPs pertaining to SM are ACP 194, Policy for the Coordination of Military Radio Frequency Allocations and Assignments Between Cooperating Nations, and ACP 190, Guide to Spectrum Management in Military Operations, which has been supplemented by both the US and NATO.

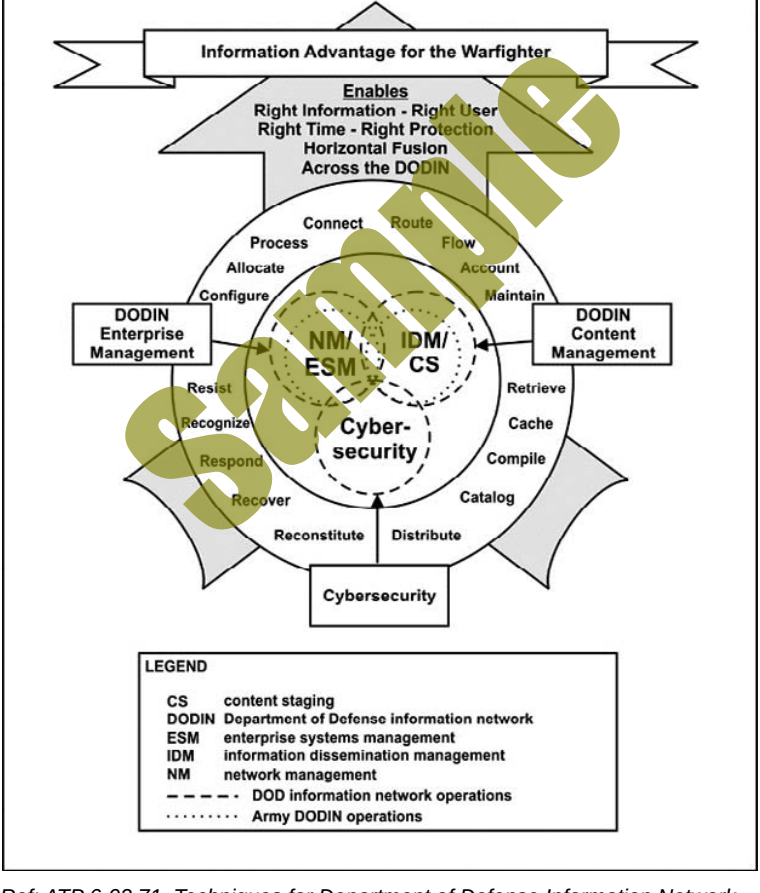
Refer to CCEB Publication 1 for a full description of the organization and mission of the CCEB.

I. Dept of Defense Info Network (DODIN) Ops

Ref: ATP 6-02.71, Techniques for Department of Defense Information Network Operations (Apr '19), chap. 1.

Department of Defense information network (DODIN) 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 (JP 3-12).

Dept of Defense Information Network (DODIN) Operations



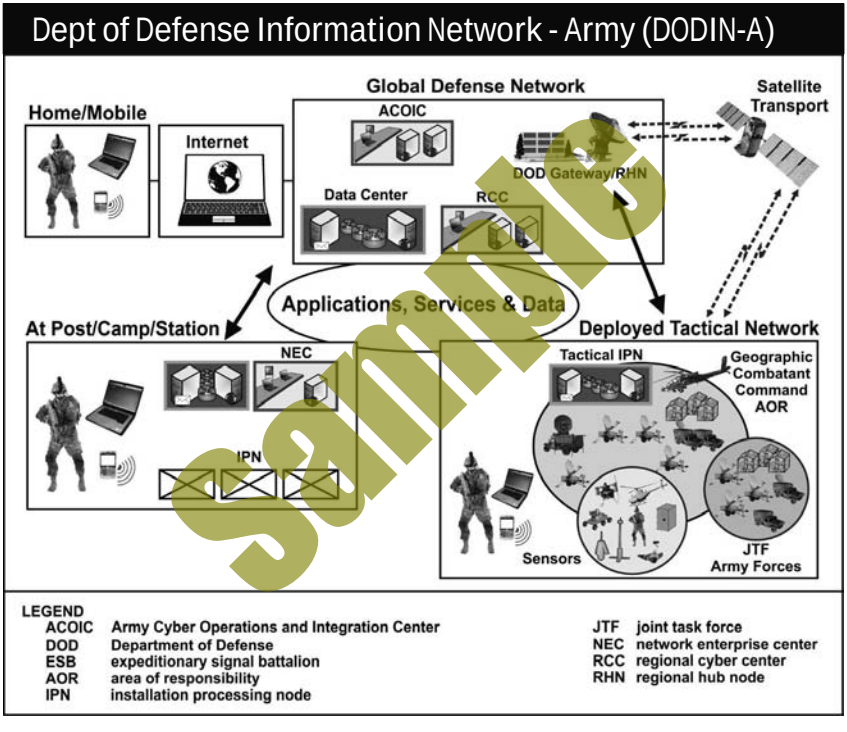
Ref: ATP 6-02.71, Techniques for Department of Defense Information Network Operations (Apr '19), fig. A-1. DODIN Operational Construct.

DODIN operations are one of the three cyberspace missions. The other cyberspace missions are defensive cyberspace operations and offensive cyberspace operations.

II. Department of Defense Information Network Operations in Army Networks (DODIN-A)

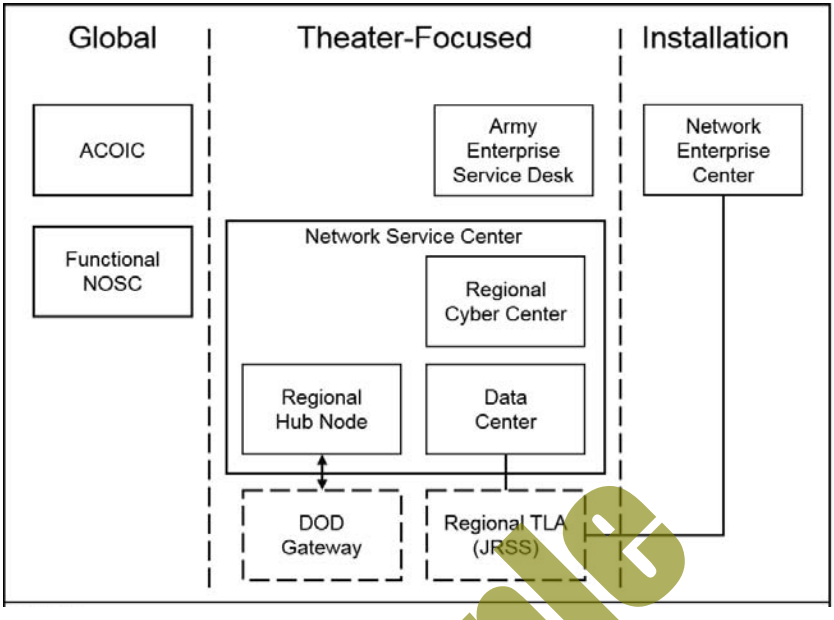
Ref: ATP 6-02.71, Techniques for Department of Defense Information Network Operations (Apr '19), pp. 1-8 to 1-9.

The Army conducts distributed DODIN operations within the DODIN-A, from the global level to the tactical edge. DODIN operations personnel install, operate, maintain, and secure from post, camp, or station to deployed tactical networks. DODIN operations provide assured and timely network-enabled services to support DOD warfighting, intelligence, and business missions across strategic, operational, and tactical boundaries. DODIN operations enable system and network availability, information protection, and information delivery.



Ref: ATP 6-02.71, Techniques for Department of Defense Information Network Operations (Apr '19), fig. 1-2. Department of Defense information network-Army.

Army personnel implement enterprise DODIN operations through an established hierarchy. The DODIN-A enables access to the right information at the right place and time, so commanders, staffs, Soldiers, civilians, and joint, inter-organizational, and multinational mission partners can meet mission requirements. The DODIN-A segments are home or mobile; post, camp, or station; and deployed tactical network. These segments allow operating and generating forces to access centralized resources from any location during all operational phases. Network support is available at the home post, camp, or station and throughout the deployment cycle.



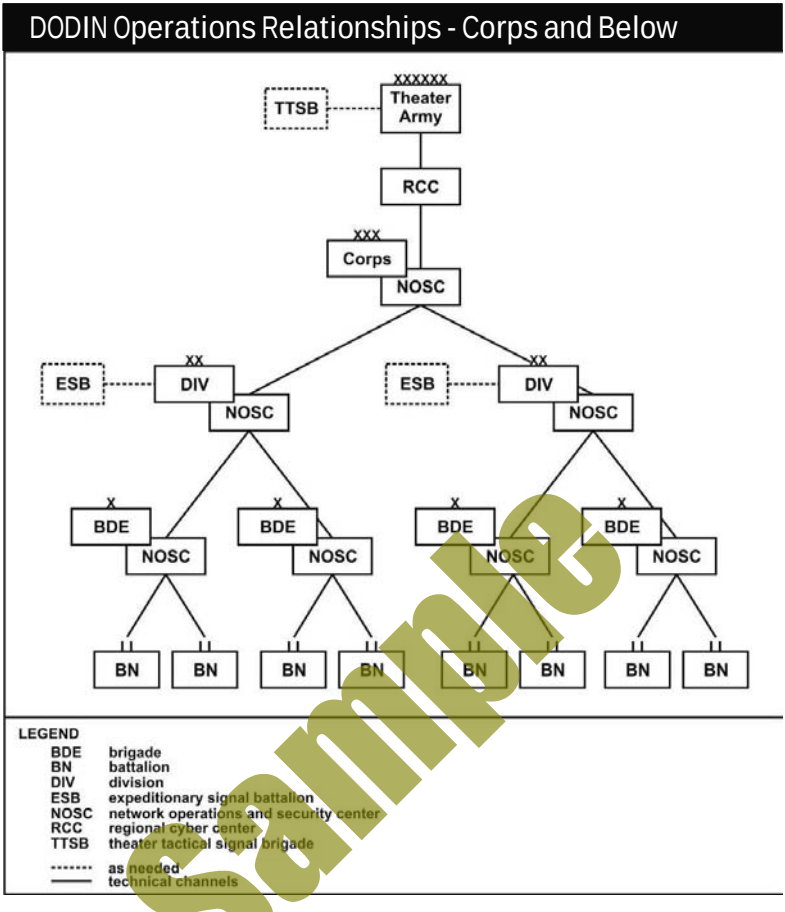
The network service center includes data centers, DOD gateway facilities, and regional hub nodes. The network service center is the DODIN-A interface that connects Army users with joint services and applications. The network service center includes both joint and Army-unique capabilities. The DOD gateway and long-haul satellite transport are joint capabilities that provide backbone connectivity and connection to DISN services. The data center and regional hub node are Army capabilities. The regional hub node provides the connection between deployed Army enclaves and the DODIN.

For more information about the regional hub node, refer to ATP 6-02.60. For more information on DOD gateway, refer to JP 6-0 and ATP 6-02.54.

The data center provides a data repository for content staging, continuity of operations, and redeployment support. It also provides access for those users who access the network from home or a temporary duty location.

The post, camp, and station segment is the primary network access point while in garrison. The post, camp, and station segment connects through the data center and provides access to the other network segments in both secure and nonsecure modes. The post, camp, and station segment allows users to train, collaborate, and conduct mission rehearsals. The installation processing node hosts enterprise services and applications associated with garrison operations. The installation processing node also connects users to installation-level services. The local NEC centrally manages these services. Applications and services within installation processing nodes provide either a temporary processing center presence until data center service is available or a permanent computing presence where technical or operational considerations dictate.

The deployed tactical network enables real-time employment of battle command common services, automated information systems, and information collection assets by deployed forces. The deployed tactical network enables the GCC and commander, joint task force (CJTF) to conduct joint, distributed operations with units in dispersed geographic locations. It allows commanders to conduct collective training with their units. The deployed tactical network connects to the DOD gateway to access DISN services, and to facilitate data replication at the data center for continuity of operations. This allows the unit to maintain its operational tempo with minimal mission impact.



Ref: ATP 6-02.71 (Apr '19), fig. 2-3. Department of Defense information network operations relationships-corps and below.

Corps and Division G-6

G-6 sections in the corps and division are organized the same, except the grade structure. The G-6 controls DODIN operations within the unit's area of operations in compliance with joint, Army, and theater policies. The G-6 works closely with the higher headquarters G-6 or J-6, subordinate G-6, battalion or brigade signal staff officer (S-6), OPCON theater tactical signal brigade or ESB elements, and the organic signal, intelligence, and sustainment company to achieve integrated DODIN operations supporting the commander's intent. The G-6 staff plans and designs DODIN operations capabilities and support for command posts and subordinate units. The staff also provides training and readiness oversight for assigned and attached units.

The G-6 controls and monitors the network situational awareness view, including subordinate networks. The G-6 also helps integrate the network situational awareness view with that of the higher headquarters, for example the one controlled and maintained by a joint task force J-6. The situational awareness view consists of the status of all network components within the unit's area of operations, as well as the status of WAN links to theater, adjacent, and subordinate units. 2-69. Commanders have the authority to delay directed changes to their portion of the network. The com-

mander may receive a network directive from higher headquarters that could adversely impact the unit's mission. In this case, issues will be resolved through command channels. Issue resolution requires close coordination between the commander, the G-6, and the higher headquarters commander and G-6 or J-6. The commander carefully considers the potential impact of delayed compliance with network directives and coordinates with higher headquarters and affected organizations to resolve compatibility issues and comply with the directed changes as soon as the tactical situation allows.

The G-6 section provides DODIN operations support to the main, tactical, and support area command posts and the mobile command group. G-6 DODIN operations activities integrate geographically separated units into the DODIN-A. Subordinate units' DODIN operations provide another level of management, which the G-6 coordinates as part of the overall DODIN operations plan.

Units without organic signal assets, such as functional support brigades, sometimes augment corps and divisions. The supported headquarters provides communications support for augmenting units, either with elements of their organic signal company or by requesting external, pooled assets through the request for forces process. The G-6 integrates the supporting brigade and other signal assets into the network and provides DODIN operations for the supporting unit. The expanded DODIN operations mission may require augmenting the DODIN operations section with external capabilities from the supporting unit S-6 or from a theater tactical signal brigade or ESB.

The corps or division G-6 has these DODIN operations responsibilities—

- Recommending communications system and DODIN operations priorities for networks and systems to support the commander's priorities.
- Establishing procedures for relevant information and information systems to develop the common operational picture, in coordination with the assistant chief of staff, operations.
- Managing IT infrastructure to follow theater and Army-wide policies and standards, in coordination with the SC(T).
- Serving as the Army component G-6 in a joint task force, when designated. This mission may require equipment and personnel augmentation and support from the SC(T) and RCC.
- Serving as the joint task force J-6, if designated. This mission may require equipment and personnel augmentation.
- Advising the commander, staff, and subordinate commanders on communications networks and information services.
- Supervising DODIN operations in the area of operations.
- Monitoring, and making recommendations for, communications networks and information services.
- Preparing, maintaining, and updating communications systems operation estimates, plans, and orders. These orders often require configuration management changes across multiple organizations.
- Providing signal units with direction and guidance for plans and diagrams to establish the information network.
- Providing signal units with unit locations, organizational status, and communications requirements.
- Planning the integration of information systems.
- Developing, updating, and distributing signal operating instructions.
- Coordinating with signal elements of higher, adjacent, subordinate, and multinational units.
- Preparing and publishing communications system standard operating procedures for command posts.

Chap 7

I. Cybersecurity Fundamentals

Ref: ATP 6-02.71, Techniques for Department of Defense Information Network Operations (Apr '19), pp. A-7 to A-15.

The Army depends on reliable networks and systems to access critical information and supporting information services to accomplish their missions. Threats to the DODIN exploit the increased complexity and connectivity of Army information systems and place Army forces at risk. Like other operational risks, cyberspace risks affect mission accomplishment. They can increase the needed time and space to conduct operations, or decrease a unit's performance or effectiveness. DOD networks experience adversary cyberspace attacks every day. Robust cybersecurity measures prevent adversaries from accessing the DODIN through known vulnerabilities. The cybersecurity measures apply to general threats and known vulnerabilities, as opposed to specific attacks.

Cybersecurity ensures IT assets provide mission owners and operators confidence in the confidentiality, integrity, and availability of information systems and information, and their ability to make choices based on that confidence. The DOD cybersecurity framework (see DODI 8500.01) provides the foundation for cybersecurity.

Cybersecurity supports effective operations in cyberspace where—

- Missions and operations continue under any cyberspace threat situation or condition.
- IT components of weapons systems and other defense platforms function as designed and adequately meet operational requirements.
- The DODIN collectively, consistently, and effectively defends itself.
- The information network securely and seamlessly extends to mission partners.
- U.S. forces and mission partners can access their information and command and control channels, but their adversaries cannot.

DOD cybersecurity complies with National Institute of Standards and Technology security and risk management publications to ensure mission partner interoperability. These publications are available online at the National Institute of Standards and Technology Computer Security Resource Center.

The cybersecurity framework consists of—

- Cybersecurity risk management
- Operational resilience
- Integration and interoperability
- Cyberspace defense
- Cybersecurity performance
- DOD information
- Identity assurance
- IT
- Cybersecurity workforce
- Mission partners

Risk Management Framework

Ref: ATP 6-02.71, Techniques for Department of Defense Information Network Operations (Apr '19), pp. A-9 to A-11.

The risk management framework (formerly the DOD Information Assurance Certification and Accreditation Process) provides a disciplined and structured process for combining information systems security and risk management into the system development life cycle. The DOD risk management framework complies with National Institute of Standards and Technology guidelines to align with federal civilian agencies. The risk management framework has six steps—

1. Categorize System

- Describe the system, including the system boundary, and document the description in the security plan.
- Register the system with the DOD Component cybersecurity program.
- Assign qualified personnel to risk management framework roles.

2. Select Security Controls

- Identify common controls.
- Identify the security control baseline for the system and document in the security plan.
- Develop and document a system-level strategy for continuously monitoring the effectiveness of security controls and proposed or actual changes to the system and its operating environment.
- Develop and implement processes whereby the authorizing official reviews and approves the security plan and system-level continuous monitoring strategy.

3. Implement Security Controls

- Implement security controls specified in the security plan in accordance with DOD implementation guidance.

4. Assess Security Controls

- Develop, review, and approve a plan to assess security controls using a methodology consistent with National Institute of Standards and Technology Special Publication 800-30.
- Assess security controls in accordance with the security assessment plan and DOD assessment procedures.
- Record the compliance status of security controls.
- Assign vulnerability severity value for security controls.
- Determine risk level for security controls.
- Assess and characterize the aggregate level of risk to the system.

5. Authorize System

- Prepare the program of action and milestones based on the vulnerabilities identified during the security control assessment.
- Assemble the security authorization package and submit to the authorizing official for adjudication.
- Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

- Decide whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.
- If the risk is determined to be unacceptable, issue a denial of authorization to operate. If the system is already operational, the authorizing official will issue a denial of authorization to operate and stop operation of the system immediately.

6. Monitor Security Controls

- Determine the security impact of proposed or actual changes to the information system or platform IT system and its environment of operation.
- Assess a subset of the security controls employed within and inherited by the information system or platform IT system in accordance with the system-level continuous monitoring strategy.
- Conduct remediation actions based on the results of ongoing monitoring activities, risk assessment, and outstanding items in the program of action and milestones.
- The program manager or system manager updates the security plan and program of action and milestones, based on the results of the system-level continuous monitoring process. The information system security manager may recommend changes or improvements to the implementation of assigned security controls, the assignment of additional security controls, or changes or improvements to the design of the system to the security control assessor and authorizing official.
- Report the security status of the system, including the effectiveness of security controls, to the authorizing official and other appropriate organizational officials, in accordance with the monitoring strategy.
- The authorizing official continues to review the reported security status of the system, including the effectiveness of security controls, in accordance with the monitoring strategy, to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.
- Implement a system decommissioning strategy, when needed. The decommissioning strategy defines the actions required when removing an information system or platform IT system from service.

Cybersecurity Reciprocity

Cybersecurity reciprocity aids rapid, efficient IT capability development and fielding. Reciprocity reduces redundant testing, assessment, and documentation, and the associated costs in time and resources. The risk management framework presumes acceptance of existing test and assessment results and authorization documentation from other Services and federal agencies.

The Services share security authorization packages and agree to accept other Services' test and assessment results and authorization to support cybersecurity reciprocity. Reciprocal acceptance of DOD and other federal agency and department security authorizations ensures interoperability and reduces redundant testing. It is important that each Service exercises due diligence in assessing, documenting, and approving systems, software, and configurations, since all Services share a risk accepted by one Service.

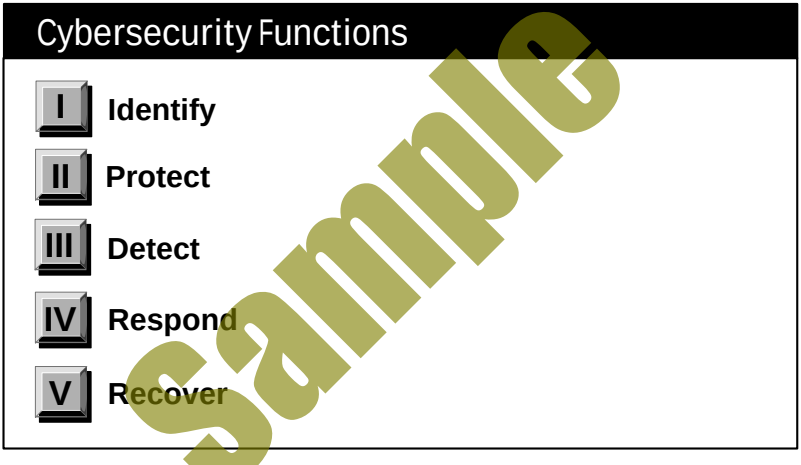
Refer to DODI 8510.01 for detailed, authoritative guidance on implementing the risk management framework.

II. Cybersecurity Functions

Ref: ATP 6-02.71, Techniques for Department of Defense Information Network Operations (Apr '19), pp. A-16 to A-25.

Cybersecurity includes both technical and non-technical measures, such as risk management, personnel training, audits, and continuity of operations planning. Cybersecurity factors in all cyber incidents that occur through malicious or accidental activity by enemy, adversary or friendly entities.

Cybersecurity functions help an organization manage risk by organizing information, enabling risk management decisions, mitigating threats, and improving security by learning from earlier activities. These functions align with existing incident management methodologies and help show the impact of cybersecurity measures.



Cybersecurity personnel perform these functions concurrently and continuously to mitigate the dynamic cyberspace risk.

I. Identify

The identify function develops situational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. This function helps cybersecurity personnel understand the mission, the resources supporting critical functions, and related cybersecurity risks. This understanding allows an organization to focus and prioritize its efforts, consistent with its risk management strategy and mission needs.

A. Identify Mission-Critical Assets

Mission-critical assets are those resources without which the unit's key missions would significantly degrade or cease to function. The steps are—

- Inventory the organization's physical devices, systems, and software applications.
- Map the associated communication and data flows.
- Understand cybersecurity roles and responsibilities of higher & subordinate units.
- Identify the security categories for resources.

Tools of Cyber Attacks

Ref: DCSINT Handbook No. 1.02, Critical Infrastructure (Aug '06), pp. IV-9 to IV-11.

Backdoor

This is used to describe a back way, hidden method, or other type of method of by passing normal security in order to obtain access to a secure area. It is also referred to as a trapdoor. Sometimes backdoors are surreptitiously planted on a network element; however, there are some cases where they are purposely installed on a system.

Denial of Service Attacks (DOS)

A DOS attack is designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash. An even more effective DOS is the distributed denial of service attack (DDOS). This involves the use of numerous computers flooding the target simultaneously. Not only does this overload the target with more requests, but having the DOS from multiple paths makes backtracking the attack extremely difficult, if not impossible. Many times worms are planted on computers to create zombies that allow the attacker to use these machines as unknowing participants in the attack. To highlight the impact of these type attacks, in February 2000, DOS attacks against Yahoo, CNN, eBay and other e-commerce sites were estimated to have caused over a billion dollars in losses. DOS attacks have also been directed against the military. In 1999, NATO computers were hit with DOS attacks by hactivists protesting the NATO bombing in Kosovo.

E-mail Spoofing

E-mail spoofing is a method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source. This method is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). For example, e-mail could be sent claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

IP Address Spoofing

A method that creates Transmission Control Protocol/Internet Protocol (TCP/IP) packets using somebody else's IP address. Routers use the "destination IP" address to forward packets through the Internet, but ignore the "source IP" address. This method is often used in DDOS attacks in order to hide the true identity of the attacker.

Keylogger

A software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the actual keys being typed, a user can easily obtain passwords and other information the computer operator may not wish others to know.

Logic Bomb

A program routine that destroys data by reformatting the hard disk or randomly inserting garbage into data files. It may be brought into a computer by downloading a public-domain program that has been tampered with. Once it is executed, it does its damage immediately, whereas a virus keeps on destroying.

Physical Attacks

This involves the actual physical destruction of a computer system and/ or network. This includes destroying transport networks as well as the terminal equipment.

Sniffer
A program and/or device that monitors data traveling over a network. Although sniffers are used for legitimate network management functions, they also are used during cyber attacks for stealing information, including passwords, off a network. Once emplaced, they are very difficult to detect and can be inserted almost anywhere through different means.

Trojan Horse
A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed performs a function in the background such as allowing other users to have access to your computer or sending information from your computer to other computers.

Viruses
A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. There are different types of viruses. Some of these are:

- **Boot Sector Virus:** Infects the first or first few sectors of a computer hard drive or diskette drive allowing the virus to activate as the drive or diskette boots.
- **Companion Virus:** Stores itself in a file that is named similar to another program file that is commonly executed. When that file is executed the virus will infect the computer and/or perform malicious steps such as deleting your computer hard disk drive.
- **Executable Virus:** Stores itself in an executable file and infects other files each time the file is run. The majority of all computer viruses are spread when a file is executed or opened.
- **Overwrite Virus:** Overwrites a file with its own code, helping spread the virus to other files and computers.
- **Polymorphic Virus:** Has the capability of changing its own code allowing the virus to have hundreds or thousands of different variants making it much more difficult to notice and/or detect.
- **Resident Virus:** Stores itself within memory allowing it to infect files instantaneously and does not require the user to run the “execute a file” to infect files.
- **Stealth Virus:** Hides its tracks after infecting the computer. Once the computer has been infected the virus can make modifications to allow the computer to appear that it has not lost any memory and or that the file size has not changed.

Worms
A destructive software program containing code capable of gaining access to computers or networks and once within the computer or network causing that computer or network harm by deleting, modifying, distributing, or otherwise manipulating the data.

Zombie
A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a Distributed Denial of Service attack (DDOS).

See pp. 0-2 to 0-5 for an overview of the global cyber threats and cyber attacks against the U.S. See previous pages (pp. 7-16 to 7-17) and 7-26 to 7-27 for an overview of the cyber threat activities. See also p. 2-24 for discussion of threats in cyberspace from FM 3-12.

Chap 8

I. Acronyms & Abbreviations

A

ACOIC	Army Cyber Operations and Integration Center
AOC	air operations center
AOR	area of responsibility
ARCYBER	U.S. Army Cyber Command
ARFOR	Army forces
ASCC	Army Service component command
ASM	Army Spectrum Manager
ASMO	Army Spectrum Management Office
ATO	air tasking order

C

CCDR	combatant commander
CCMD	combatant command
CCMF	Cyber Combat Mission Force
CEMA	cyber electromagnetic activities
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-HQ	Cyber National Mission Force Headquarters
CNO	computer network operations
CO	cyberspace operations
CO-IPE	cyberspace operations-integrated planning element
COMSEC	communications security
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

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
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DODIN	Department of Defense information network
DODIN-A	Department of Defense information network -Army
DSO	Defense Spectrum Organization

E

E3	electromagnetic environmental effects
EA	electronic attack
EARF	electronic attack request format
EM	electromagnetic
EME	electromagnetic environment
EMOE	electromagnetic operational environment
EMP	electromagnetic pulse
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EOB	electromagnetic order of battle
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
EWC	electronic warfare cell
EWE	electronic warfare element
EWO	electronic warfare officer
EXORD	execute order

F

FAS	frequency assignment subcommittee
FM	frequency management

Chap 8

(CYBER1) II. Glossary

Editor's Note. This combined joint and Army glossary lists pertinent cyberspace and electromagnetic spectrum-related terms as provided from the primary references used to compile the CYBER1 SMARTbook, to include JP 3-12 (2018), FM 3-12 (2017), ATP 3-36 (2014), JP 6-01 (2012), and ATP 6-20.71 (2019). The cited publication precedes the definition in parenthesis, whereas the proponent publication for terms is listed in parentheses after the definition. In cases of duplicate definitions (across multiple references), the primary or most up-to-date (current) definition is provided.

A

Aimpoint. (FM 3-12) A point associated with a target and assigned for a specific weapon impact. (JP 3-60)

Army design methodology. (FM 3-12) A methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them. (ADP 5-0)

C

configuration management. (ATP 6-21.7) A discipline applying technical and administrative direction and surveillance to: (1) identify and document the functional and physical characteristics of a configuration item; (2) control changes to those characteristics; and (3) record and report changes to processing and implementation status. (JP 6-0)

Countermeasures. (FM 3-12) 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 3-13.1)

critical infrastructure protection. (ATP 6-21.7) Actions taken to prevent, remediate, or mitigate the man-made or natural risks to critical infrastructure and key assets. (JP 3-28)

cross domain solution. (ATP 6-21.7) A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

cyber electromagnetic activities. (ATP 3-36). 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. (ADRP 3-0)

cyber incident. (ATP 6-21.7) Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. (CNSSI 4009)

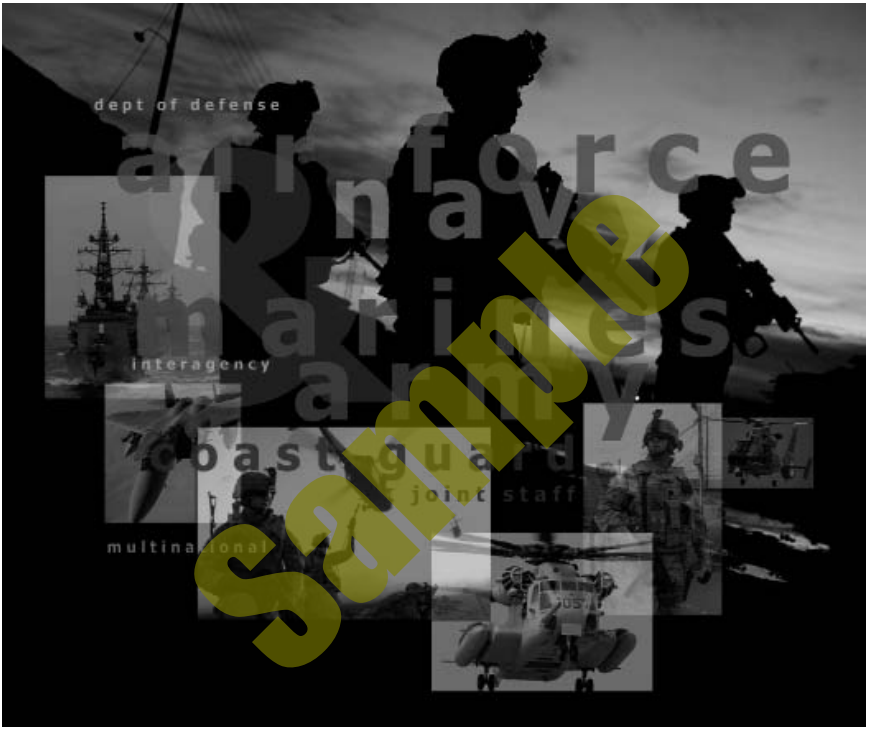
cybersecurity. (ATP 6-21.7) Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)

cyberspace. (JP 3-12) 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. (DOD Dictionary. Source: JP 3-12)

(CYBER1) Index

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.

SMARTbooks
INTELLECTUAL FUEL FOR THE MILITARY

MILITARY REFERENCE: JOINT & SERVICE-LEVEL

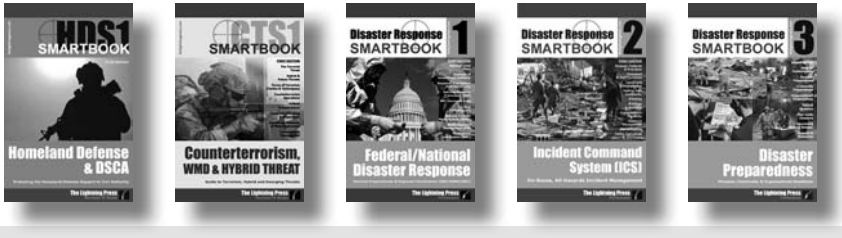
Recognized as a "whole of government" doctrinal reference standard by military professionals around the world, SMARTbooks comprise a comprehensive professional library.

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.

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.

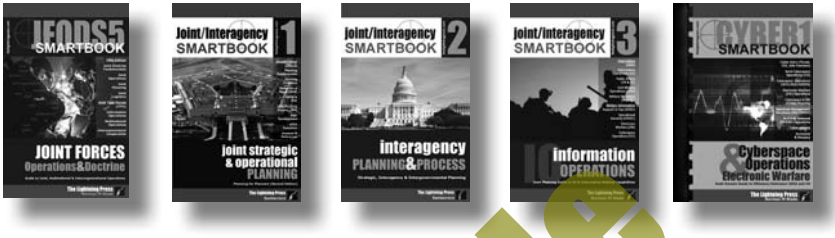


The Lightning Press is a **service-disabled, veteran-owned small business,** DOD-approved vendor and federally registered — to include the SAM, WAWF, FBO, and FEDPAY.

RECOGNIZED AS THE DOCTRINAL REFERENCE STANDARD BY MILITARY PROFESSIONALS AROUND THE WORLD.

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.



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.

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).

Purchase/Order

www.TheLightningPress.com

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

Email: SMARTbooks@TheLightningPress.com

Phone Orders, Customer Service & Quotes

Live customer service and phone orders available
Mon - Fri 0900-1800 EST at (863) 409-8084

24-hour Order/Voicemail

Record your order (or request a call back)
by voicemail at 1-800-997-8827

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** (GCPC/GPC) and **Purchase Orders** (PO/PR&Cs).

15% OFF
RETAIL EVERYDAY

Buy direct from our website and always get the latest editions and the best pricing. Join our SMARTnews email list for free notification of changes and new editions.

www.TheLightningPress.com

CYBER1

thelightningpress.com

(CYBER1) The Cyberspace Operations & Electronic Warfare SMARTbook

Multi-Domain Guide to Offensive/ Defensive CEMA and CO

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.

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 DoD information network (DODIN) operations.

Electronic warfare (EW) is any 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: electronic attack, electronic protection, and electronic warfare support.

DIME is our DOMAIN!™

SMARTbooks: Reference Essentials for the Instruments of National Power

Part of our "Military Reference" Series

ISBN 9781935886716
90000 >
9 781935 886716