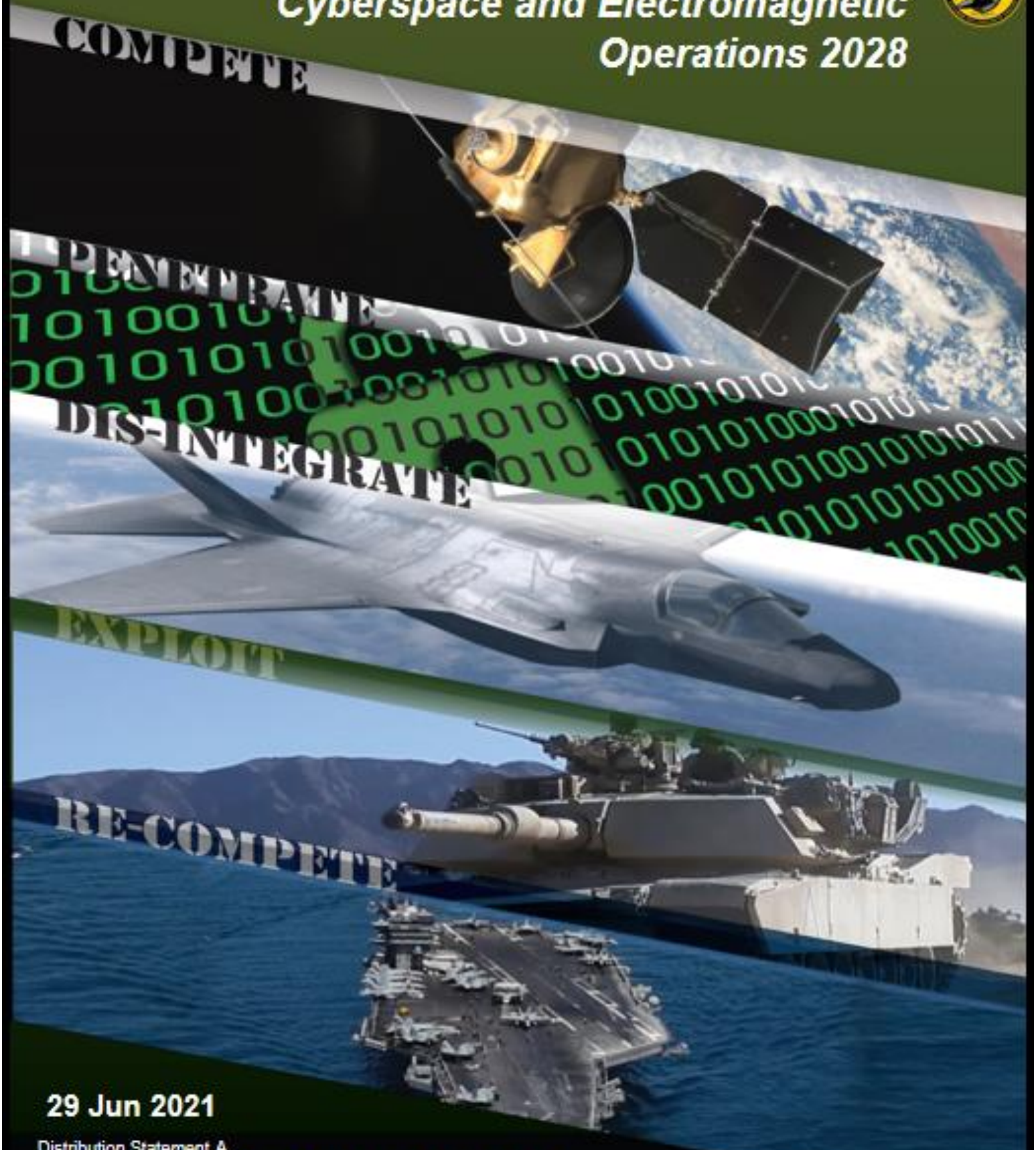
AFC Pamphlet 71-20-8

Army Futures Command Concept for Cyberspace and Electromagnetic Operations 2028



29 Jun 2021

This page intentionally left blank

Executive Summary

AFC Pamphlet 71-20-8, The *Army Futures Command Concept for Cyberspace and Electromagnetic Warfare Operations*, addresses applications and ideas for the conduct and integration of cyberspace and electromagnetic warfare operations. Cyberspace and electromagnetic warfare operations are the employment of cyberspace and electromagnetic warfare capabilities where the primary purpose is to achieve objectives in or through cyberspace and the electromagnetic spectrum. Cyberspace and electromagnetic operations use integrated cyberspace and electromagnetic warfare capabilities, scalable cyberspace and electromagnetic warfare formations, and cyberspace infrastructure to provide effects within and across all domains, the electromagnetic spectrum and the information environment through the coordination and application of their own unique capabilities to support multi-domain operations. Additionally, these solutions are an integration and synchronization mechanism that provide enabling support to the convergence of all warfighting capabilities and information related capabilities across time, space, and scale to create windows of superiority.

The Army will continually develop capabilities commensurate with the dynamic nature of cyberspace, the electromagnetic environment, and evolving threats to achieve freedom of action in all domains and the information space through the conduct of cyberspace and electromagnetic warfare operations in support of multi-domain operations. Subsequently, this concept will remain a living document that strives to keep pace with rapidly evolving cyberspace and electromagnetic warfare technical innovations as well as the national, joint, and Army policy change decisions.

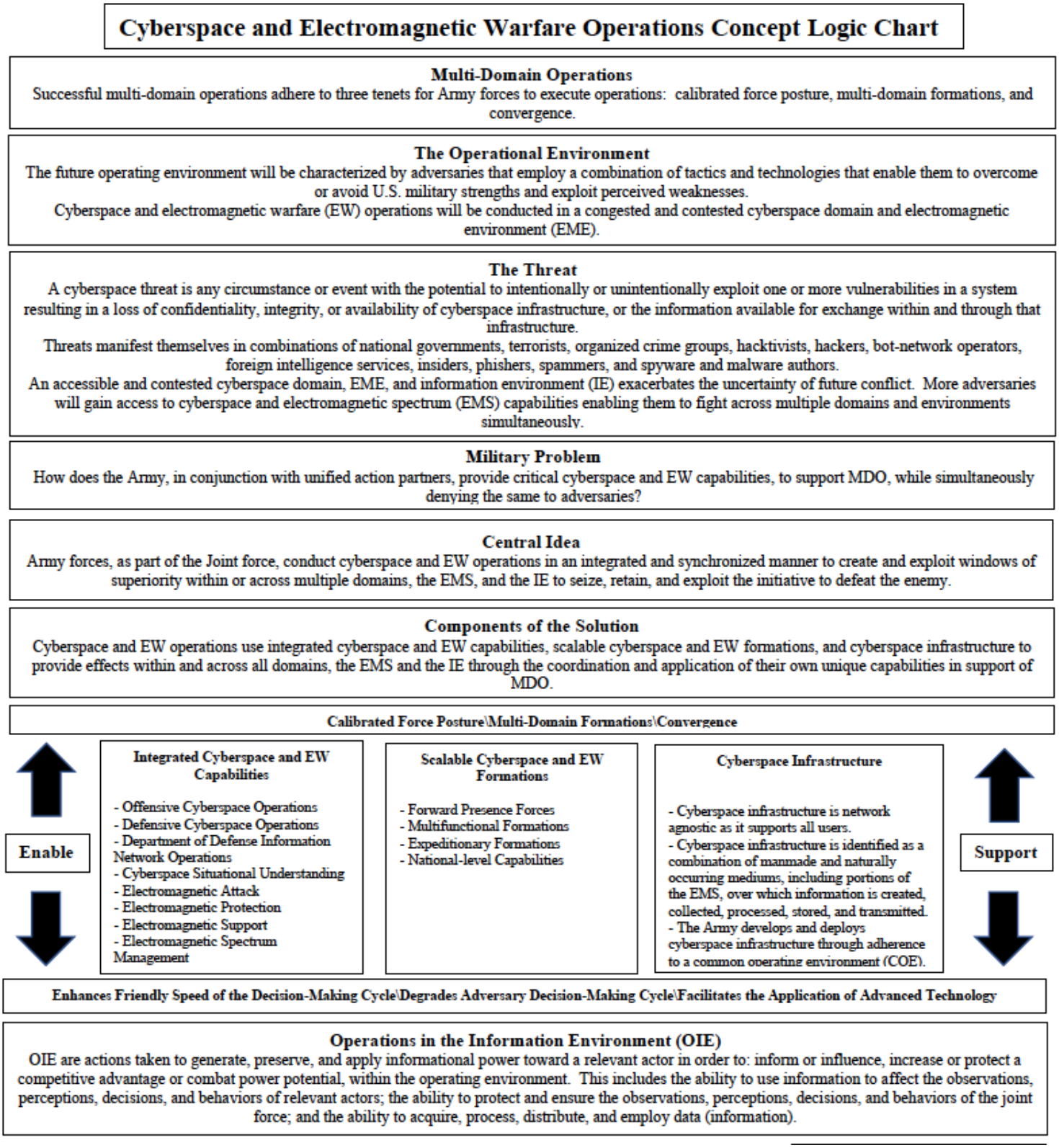


Figure 1. Cyberspace and EW Operations Logic Chart

U.S. Army Futures Command
Futures and Concepts Center
Austin, TX 78701-2982

29 June 2021

Force Management

ARMY FUTURES COMMAND CONCEPT FOR CYBERSPACE AND ELECTROMAGNETIC WARFARE OPERATIONS

D. SCOTT MCKEAN
Lieutenant General, USA
DCG, Army Futures Command

History. This document is a new U.S. Army Futures Command (AFC) pamphlet that supersedes the United States (U.S.) Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-8-6 dated 9 January 2018.

Summary. This pamphlet describes how the Army will operate in and through cyberspace and the electromagnetic spectrum and fully integrate cyberspace, electromagnetic warfare (EW), and operations in the information environment (OIE) in support of multi-domain operations to meet future operational challenges.

Applicability. This pamphlet applies to all Department of the Army activities that identify and develop doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) solutions to support cyberspace and electromagnetic spectrum operations initiatives. Active Army, Army National Guard, and U.S. Army Reserve forces may use this pamphlet to identify future cyberspace and electromagnetic spectrum operations trends in the Army. This concept should also serve as the primary cyberspace and EW operations reference for war games, experimentation, and innovation aimed at maintaining the U.S. Army as the preeminent ground force in the world.

Proponent and supplementation authority. The proponent of this pamphlet is the Army Futures Command Headquarters, Director, Futures and Concepts Center (FCC). The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. Do not supplement this pamphlet without prior approval from Director, Futures and Concept Center, 210 West 7th Street, Austin, TX 78701-2982.

Suggested improvements. Users are invited to submit comments and suggested improvements via DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Director, Futures and Concept Center (FCFC-CE), 210 West 7th Street, Austin, TX 78701-2982.

Availability. This pamphlet is available on the FCC homepage at https://www.army.mil/futuresandconceptscenter#org-resources.

Summary of Change

AFC Pamphlet 71-20-8
Army Futures Command Concept for Cyberspace and Electromagnetic Warfare 2028

This revision:

- Aligns cyberspace and EW capabilities within an information focused operational framework.
- Emphasizes cyberspace and EW support to operations in the information environment (OIE).
- Establishes and defines the concept of cyberspace infrastructure.
- Identifies portions of the electromagnetic spectrum (EMS) as a component of cyberspace infrastructure.
- Proposes defining the conditions, circumstances, and influences that affect the employment and application of advanced technology as an environment similar to other unique operating environments.

Contents

Figures List

Chapter 1
Introduction

1-1. Purpose

a. This revision to *The Army Futures Command Concept for Cyberspace and Electromagnetic Warfare Operations*, addresses applications and ideas for conducting and integrating cyberspace and electromagnetic warfare (EW) operations. This concept describes employing cyberspace and EW operations as an integrated and synchronized system in support of Multi-Domain Operations (MDO). Cyberspace and EW systems provide significant points of presence on the battlefield and can be used as delivery platforms for precision engagements. This concept identifies the Army's required cyberspace and EW capabilities.

b. Cyberspace and EW operations are essential to the successful execution of MDO. While cyberspace and EW sometimes differ in their employment and tactics, their functions and capabilities must be integrated and synchronized to maximize their effects. Cyberspace and EW operations include Department of Defense information network operations (DODIN), defensive cyberspace operations (DCO) and offensive cyberspace operations (OCO). EW consists of electromagnetic attack (EA), electromagnetic protect (EP), and electromagnetic warfare support (ES). When discussing the DODIN, this concept addresses the Army's portion of the DODIN as DODIN-A.

c. Army forces have integrated and synchronized cyberspace and EW capabilities along with the authorities to conduct effective cyberspace and EW operations as part of an overall combined arms strategy in support of MDO. Cyberspace and EW operations provide the capability to process and manage operationally relevant actions across multiple domains, the electromagnetic spectrum (EMS), and the information environment (IE). The IE is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[1] Cyberspace and EW operations allow simultaneous and linked maneuver in and through multiple domains, the EMS, and the IE, while engaging adversaries and populations directly across time, space, and scale. Cyberspace and EW operations provide commanders a full range of physical, virtual, lethal, and nonlethal capabilities tailored to enhance the combat power of Army forces conducting MDO.

d. The Army conducts cyberspace and EW operations within the IE. The ease of access to technical networks facilitates information sharing and enhances the social aspect of the IE. The dimensions of the IE are physical, virtual, and cognitive. Operations in the information environment (OIE), whether inside or outside of cyberspace, can affect friendly, neutral, and threat operations within cyberspace.

e. This concept presents a new focus on cyberspace and EW support to OIE which is described as actions taken within the operating environment to: inform or influence a relevant actor, increase and protect a competitive advantage against a relevant actor, or increase and protect combat power potential for a relevant actor. In the past, Army commands and staffs bifurcated OIE to include cyberspace, EW, and the capabilities and structures supporting them, while planning and executing

[1] Joint Publication 3-13.1 U.S. Department of Defense, *Information Operations* (Washington, DC: United States Department of Defense, 2012 Incorporating Change 1 2014)

operations. In addition, the planning and operational foci for cyberspace and EW tended to emphasize OCO and EA rather than how cyberspace and EW could enable and exploit the tactical and strategic effects of information. As such, new organizational and doctrinal paradigms are required to support the full integration and synchronization of these capabilities to maximize their effects, and to eliminate potential conceptual confusion when integrating and synchronizing information-related capabilities (IRCs) to support MDO.

1-2. References
Appendix A lists required and related publications.

1-3. Explanation of abbreviations and terms
The glossary explains abbreviations and terms used in this pamphlet.

1-4. Linkage to other concepts
This concept is consistent with cyberspace and EW requirements outlined in *TRADOC Pamphlet 525-3-1 The U.S. Army in Multi-domain Operations 2028*, which states that the Army requires a full range of cyberspace and EMS capabilities to provide commanders the ability to adapt to changing missions rapidly, conduct decentralized operations over wide areas, maintain operational freedom of maneuver, exercise command and control, and gain and maintain the initiative.

Chapter 2
The Operational Environment and Threat

2-1. Introduction

a. An operational environment (OE) is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.[2] Staffs perform tasks and missions in and through cyberspace and the EME in support of warfighting and supporting functions. Cyberspace and EW operations, in close coordination with intelligence operations, support, enable, integrate, and synchronize operations for warfighting and support functions in support of MDO.

b. The future OE will be characterized by adversaries that employ a combination of tactics and technologies that enable them to overcome or avoid U.S. military strengths and exploit perceived weaknesses. The future OE will be more unpredictable, complex, and dangerous than today. Persistent conflict continues to evolve within the cyberspace domain and the EME where a variety of opponents will continually contest multiple aspects of cyberspace and the EME with differing synchronous and asynchronous capabilities across the conflict continuum. To appreciate the role and capabilities of cyberspace and EW, it is important to understand the cyberspace domain, the information, electromagnetic, and advanced technology environments, the variables that influence these domains and environments, and the ways in which these variables affect operations.

c. The cyberspace domain. Cyberspace has characteristics that differ from air, land, maritime, and space. These characteristics affect how the Army operates and defends cyberspace

[2] Joint Publication 3-0 U.S. Department of Defense, *Joint Operations* (Washington, DC: United States Department of Defense, 2017 incorporating Change 1 2018)

infrastructure, information, information systems (to include weapon systems), and data. Most of the cyberspace domain is man-made and reliant upon powered devices to be accessible. An exception to this man-made construct concerns the EMS, which occurs naturally though still requires the use of powered devices for access and is discussed in greater detail later in this document. The cyberspace domain, unlike the other domains, is also dependent upon private sector infrastructure and technology (much of which the Army does not own or have direct control over) to be the most effective. To manage the complexity of the cyberspace domain the military has divided it into separate layers: physical, logical, and cyber-persona.[3]

Note 1: Cyberspace is divided by layers per JP 3-12 and Information is divided by dimensions as outlined in JP 3-13. Within this document when discussing layers, they will always be in reference to cyberspace. When discussing dimensions, they will always be in reference to information.

(1) The physical layer is comprised of cyberspace infrastructure (wired, wireless, cabled links, EMS links, satellite, and optical) and communications infrastructure (wires, cables, radio frequency, routers, switches, servers, and computers). However, the physical layer uses logical constructs as the primary method of confidentiality, integrity, and availability (such as, virtual private networks that tunnel through cyberspace). The physical layer is the first point of reference for determining jurisdiction and application of authorities.

(2) The logical layer consists of those elements of the network related to one another in a way that is abstract from the physical layer (that is, the form or relationships are not tied to an individual, specific path, or node). The logical layer includes various routing and switching protocols, software operating systems, services, and host applications. A simple example is any web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator.

(3) The cyber-persona layer represents yet a higher level of abstraction. It uses rules applied in the logical layer to develop a digital representation of an individual or identity. The cyber-persona layer consists of individual network users that may or may not relate directly to an actual person or entity. This layer primarily consists of data, email and internet protocol (IP) address(es), web pages, phone numbers, and other information. While one individual may have multiple cyber-personas, which can vary in the degree to which they are factually accurate, a single cyber-persona can have multiple users making attribution in cyberspace difficult.

d. Connections between the various layers of cyberspace generate a portion of the IE that is divided into three dimensions – the physical, virtual, and cognitive - and each dimension is associated with a specific layer of cyberspace.

(1) The physical dimension is composed of command and control (C2) systems and supporting infrastructure that enable individuals and organizations to conduct operations. It is the dimension where physical platforms and the networks that connect them reside. The physical dimension relies upon cyberspace infrastructure which includes, but is not limited to, fiber optic

[3] Joint Publication 3-12 U.S. Department of Defense, *Cyberspace Operations* (Washington, DC: United States Department of Defense, 2018)

cables, computers, portions of the EMS, and networking devices. The cyberspace physical layer is associated with the IE physical dimension.

(2) The virtual dimension is the place where information is collected, processed, stored, disseminated, and protected. Information is disseminated via virtual routes over physical networks and stored within virtual file systems either on the local hard drive or in the cloud. Ultimately, actions in this dimension affect the content and flow of data. The cyberspace logical layer is associated with the IE information dimension.

(3) The cognitive dimension encompasses the minds of the persons who transmit, receive, and respond to or act on information, in this dimension people think, perceive, visualize, understand, and decide. As artificial intelligence and machine learning capabilities increase, the cognitive dimension will include such functionality. The cyberspace cyber-persona layer is associated with the IE cognitive dimension.

e. To support this information paradigm, cyberspace is divided operationally into three distinct spaces designated as friendly, neutral, and adversary.[4]

Note 2: The term spaces denote operational areas within the cyberspace domain as identified in FM 3-12.

(1) Friendly (blue) cyberspace is reliant predominantly upon the DODIN-A. The DODIN-A is the Army's cyberspace infrastructure, which enables C2, fires, intelligence, and other warfighting and support functions. Blue cyberspace offers connectivity from tactical to strategic users. These cyberspace infrastructure segments enable operating and generating forces to access centralized resources from any location during operations. Analytics and visualizations focus on friendly operations in cyberspace and the EMS including network and information system status, configuration and topology, key terrain in cyberspace, and risk.

(2) Neutral (gray) cyberspace is that which is not in the direct control of friendly or adversary forces. Cyberspace connections (wired or wireless) across publicly accessible networks are viewed as gray space; however, various public and private entities install, operate, and manage all portions of cyberspace, so these networks should not be viewed as an unconstrained global common. This portion of the cyberspace domain includes private citizens, host nations, industry, and academia, along with innumerable social networks, collaborative and educational forums, peer-to-peer services, along with state, criminal, and non-state threat actors. Consequently, U.S. Army forces have limited direct control over many of the cyberspace routes and pathways they operate within. Since private industry is the primary catalyst for commercial assets and global supply chains, the Army has become increasingly reliant on providers over which the Army has no direct influence to mitigate risk effectively. The Army works with federal, state, and local partners, along with the academic and private sectors, to meet the challenge of conducting cyberspace operations.

(3) Adversary (red) cyberspace is that portion of the cyberspace domain for which cyberspace threats have continuous access to operate and conduct cyberspace operations without repercussion. Adversaries often protect this portion of the cyberspace domain by isolating it from worldwide

[4] Joint Publication 3-12 U.S. Department of Defense, *Cyberspace Operations* (Washington, DC: United States Department of Defense, 2018)

connections. Further, adversary activity in cyberspace is easily masked or hidden making attribution difficult and, in some cases, impossible to establish. In the past, only a handful of adversaries had the ability to conduct OCO against Army forces; today, a wide range of actors utilize advanced technologies that represent an inexpensive way to pose a significant threat to the Army. Adversaries' application of low-cost cyberspace capabilities can disproportionately affect Army forces that depend on cyberspace and its ability to enhance MDO. Potential adversaries see the use of cyberspace as a low cost, clandestine, and quicker method to achieve their objectives in comparison to more traditional or non-technical measures that allow operations to be conducted below the threshold of conflict.

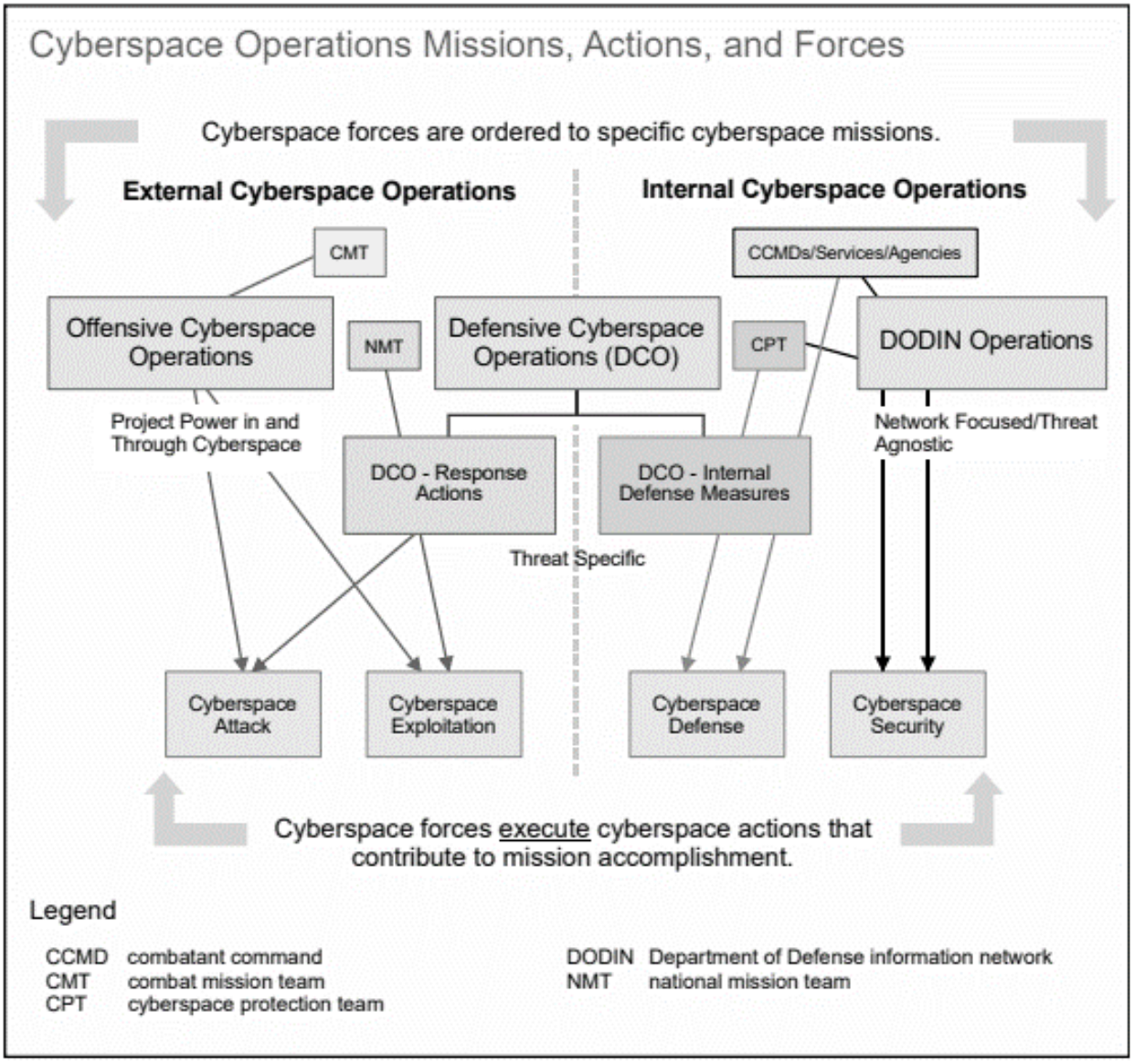


Figure 2-1. Cyberspace Operations

f. The EMS and the EME. The EMS is the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. The Army operates using the EMS in all geographic regions. The EMS is part of the EME. The EME is the resulting

product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels that may be encountered by a military force, system, or platform when performing its mission in its intended operational environment.[5] In essence, the EME is the sum of all radiated energy within a given location. Increasing usage of the EMS by military and civilian entities results in a congested and contested EME, which manifests to varying degrees throughout various operational areas.

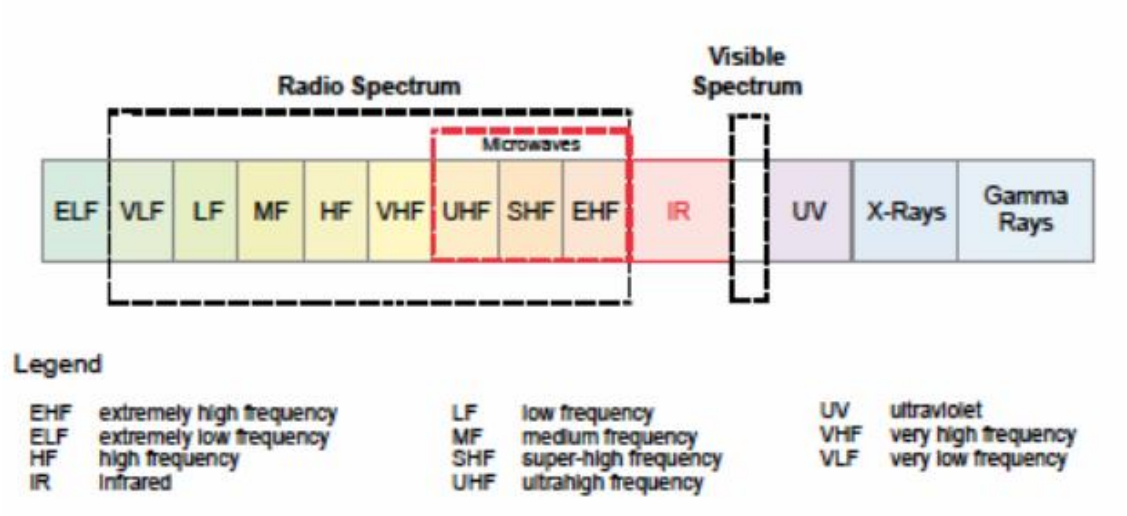


Figure 2-2. The EMS

(1) Cyberspace wireless capabilities use the EMS as a transport medium to form links in the DODIN. The Army manages its use of the EMS through spectrum management operations (SMO). SMO consist of the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic environment during all phases of military operations.

(2) Conducting SMO supports and enables the execution of cyberspace and EW operations and ensures access to the EMS in support of MDO. Synchronizing efforts between cyberspace and EW operations and other users of spectrum produces unifying and complementary efforts while minimizing conflicting effects within the EME.

(3) MDO are dependent on use of the EMS which is also a central element of the future OE for allies and adversaries. As Army forces' operational dependence on the EMS continually increases, adversaries' efforts to target this vulnerability are also increasing. The expanding ability of current and future adversaries to sense and observe electromagnetic signatures is a reality in an evolving and increasingly complex OE. Adversaries are also growing more reliant on EMS, creating vulnerabilities that result in opportunities for exploitation of their systems.

[5] Joint Publication 3-85 U.S. Department of Defense *Joint Electromagnetic Spectrum Operations* (Washington DC: United States Department of Defense, 22 May 2020)

(4) Cyberspace and the EME are becoming more congested and contested as commercial users, adversaries, partners, and the U.S. military compete for available bandwidth. Army forces cannot assume unhindered access to the cyberspace domain and the EME. Physics, technology, governing policy, and demand for bandwidth all contribute to EME congestion reducing its availability for military use. Adversary EW capabilities severely impact operational use of EMS as the Army faces determined adversaries with potent capabilities that will place it in the position of operating in a degraded EME and IE.

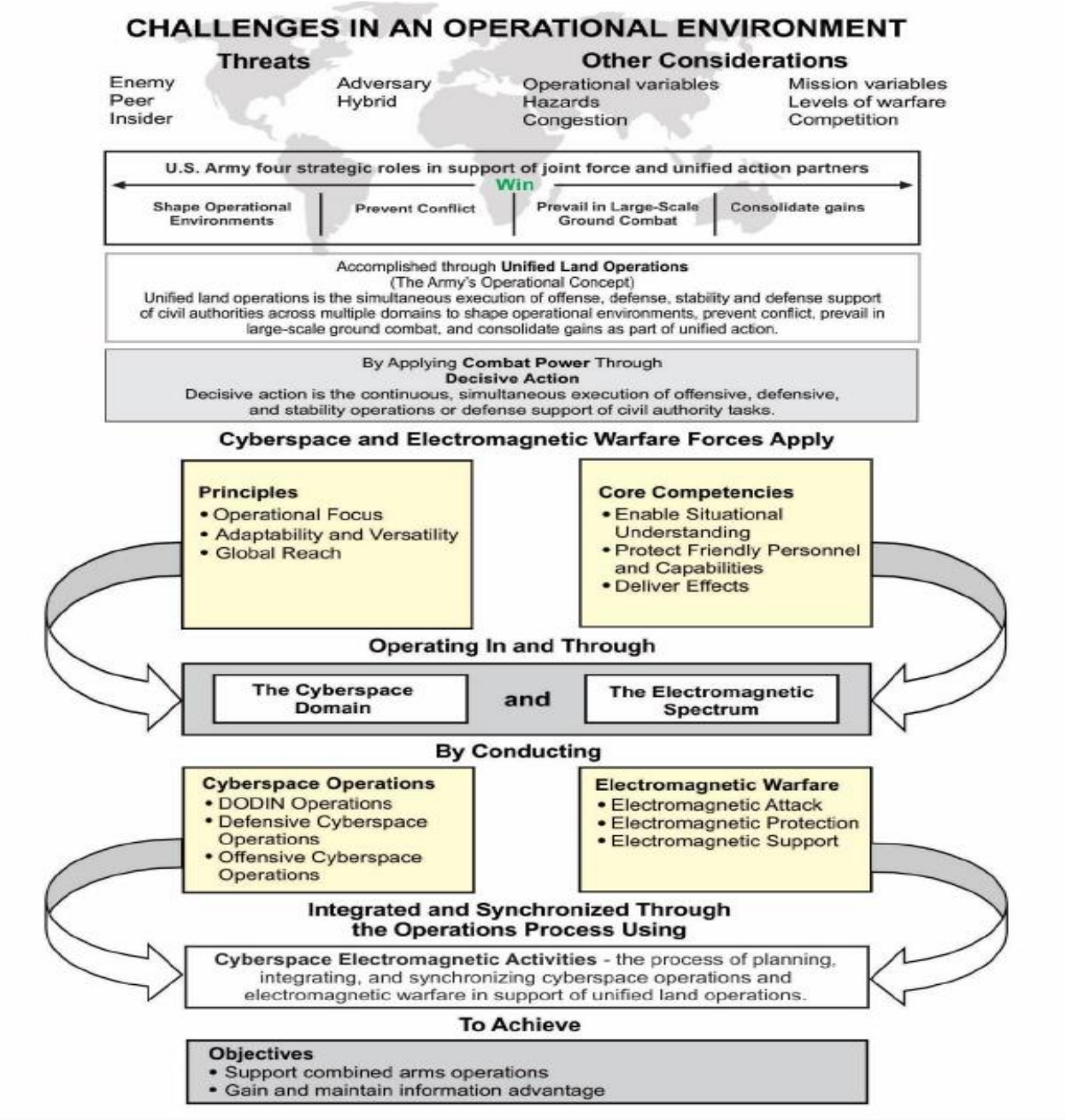


Figure 2-3. Cyberspace and EW Operations in the OE

(5) Advanced materiel properties and switching architectures have increased the speed and capacity of EMS enabling low power, near-simultaneous transmission, and jamming in the same frequency band. These developments, together with software-defined algorithms, wide-band frequency hopping, and cognitive radios, have already outpaced current practices for modeling, allocating, and managing EMS activity. Technologies such as application-specific integrated circuits, programmable logic devices, digital radio frequency memory, and shared aperture Electromagnetic attack, increase the number of ways users can exploit EMS.

(6) The shrinking size and power requirements of many EMS systems and architectures makes them more suitable for employment by remote, robotic, and autonomous systems, dramatically expanding friendly and adversary potential to conduct EW operations with small signature platforms.

g. The information environment. The IE inextricably linked to all operational environments and consists of the physical, virtual and cognitive dimensions. Information can also be considered to have two broad categories within an operational framework, the technical aspect and the cognitive aspect.

(1) During operations, the domains of air, land, maritime, space, and cyberspace are bound together by information. All these domains are constrained by the laws of physics as information is stored on physical devices and transmitted through the physical world as data by means of electrical signals, light signals, and electromagnetic waves. This represents the technical aspect of information. The cognitive aspect of information concerns the human decision-making process where factors such as inference, deduction, and reason are applied to assess, analyze, and execute. Within the context of military operations this decision-making cycle, as it relates to commanders, is known as the military decision-making process.

(2) The military decision-making process is commander focused and uses the technical components of integrated cyberspace and EW operations to maximize the speed and timeliness of information to accelerate cognitive processes to quicken the pace of the commander's decision making. Conversely, commanders use the same capabilities to undertake operations directed at slowing or lengthening an adversary's decision-making cycle. Additionally, as artificial intelligence and machine learning become more capable, the cognitive processes associated with the intellectual aspect of information will not only reside within the human mind but will also be resident as software within the technical aspect of cyberspace infrastructure adding a further layer of complexity to an already challenging process.

(3) OIE are physical, virtual, or cognitive actions taken to generate, preserve, and apply power or influence toward a relevant actor in order to: inform, shape, increase, or protect a competitive advantage or combat power potential within the operating environment. This includes the ability to use information to affect the observations, perceptions, decisions, and behaviors of relevant actors; the ability to protect and ensure the observations, perceptions, decisions, and behaviors of the joint force; and the ability to acquire, process, distribute, and employ data (information).[6]

[6] Secretary of Defense Draft Memo, *DoD Terms, and Usage Guidance for Operations in the Information Environment*, United States Department of Defense, Washington DC 2020

(a) OIE rely on the synchronization of IRCs, in concert with operations, to create effects in and through the IE. Integrated and synchronized IRCs advance the commander's intent and concept of operations; seize, retain, and exploit the initiative in the IE; and consolidate gains to achieve a decisive information advantage over the adversary.

(b) Commanders gain situational understanding of the IE through focused information operations and determine how the threat operates in that environment. Understanding begins with analyzing the threat's use of the IE and IRCs to gain an advantage. It continues with the identification of threat vulnerabilities that friendly forces can exploit or must defend against with IRCs. OIE provide commanders an implementation plan and integrative framework for employing IRCs. When employed as part of an OIE that includes multiple IRCs, cyberspace and EW operations can provide commanders an alternative solution to challenging operational problem sets.

(c) When converged with other capabilities such as long-range precision fires, space and Army Special Operations Forces (ARSOF), OIE directly supports opening and exploiting windows of superiority during competition, conflict, and return to competition. Military capabilities and IRCs that contribute to OIE include, but are not limited to, strategic communications, joint and interagency coordination, public affairs, civil-military operations, cyberspace and EW operations, cybersecurity, space operations, military information support operations, intelligence, military deception, operations security, and military and civilian engagement.

(4) Army forces will need to be able to operate in degraded cyberspace domain as well as degraded information and electromagnetic environments. In the case of a degraded IE, the definition is viewed from the user perspective, and degradation is considered in terms of the effect on information flow that influences the conduct of military operations. This approach is necessary because there is a technical and cognitive aspect to the user perspective. Physical degradation of cyberspace infrastructure may occur through a combination of configuration problems, environmental causes, or adversary activity directed against friendly cyberspace infrastructure resulting in a degraded IE. Additionally, adversary-directed disinformation campaigns and deception may be responsible for the cognitive degradation of the IE. Thus, a degraded IE is defined as any condition that adversely affects the availability, timeliness, accuracy, or integrity of information essential to the conduct of MDO.

h. Advanced technology environment. As previously stated, an operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Though not often considered as an environment, the application of advanced technology remains a unique circumstance where technology refresh cycles and innovation must be continually adapted and adopted into capability development and operational frameworks. Setting the conditions for advanced technology application, creating the circumstances that support advanced technology application, and managing the influences that the application of advanced technology has on the commander’s decision cycle are all emblematic of an operational environment. Given its conditions-based execution and cyclic pattern, advanced technology application meets the criteria as an operational environment that is crucial to execute MDO successfully. Pressure to deploy advanced technology should be balanced against the potential for increased risk and the requirements of sustained and

continuous operations. Advanced technology implementation and application should be undertaken carefully to prevent creating vulnerabilities and disrupting or degrading ongoing operations.

(1) Information and communication technology, advanced electromagnetics, bioengineering and nanotechnology all have profound effects on MDO in the coming years. Developments in these advanced technologies lead to a fighting force further enhanced by, but more profoundly dependent upon, improved robotics, remotely guided or autonomous systems, and miniaturized weapons, all supported by advanced artificial intelligence (AI) and machine learning that is more self-organizing and distributed.

(2) Cyberspace and EW operations leverage the key strategic advantage of advanced technology to enable operations in the IE while simultaneously supporting the creation of effects while identifying and selecting threats in persistently changing operational environments. Rapid identification and selection of threats will quicken attribution of malicious activity and improve the responsiveness of cyberspace and EW operations.

(3) Application of advanced technology to cyberspace and EW operations impacts the overall conduct of operations in different ways, some known or possible to foresee, others unknown and awaiting discovery. One area where the impact of advanced technology can already be felt concerns commanders' decision making and the speed of that cycle. MDO adds significant demands on headquarters staff and commanders to make decisions and translate those decisions into operational execution in a cycle that is accelerated, but which also exceeds the pace of adversary decision making and operational execution. This can be understood best by considering the way advanced technology and operations interact through operational and technological agility.

(a) Operational agility is the ability to adapt to changing operational circumstances in the execution of operations while continually incorporating change within the most accelerated decision cycle possible. Within MDO, operational agility derives its flexibility and speed from technical agility, and technical agility is derived from applying advanced technology based on varied information-related technical specialties to operational capabilities.

(b) Technical agility is the ability to adopt and incorporate advanced technology into operational capabilities with speed and precision at a quicker pace than adversary capabilities allow. Achieving technical agility is dependent upon close and comprehensive collaboration with the scientific community and industry so advanced technology can be developed, shared, and applied across a broad spectrum of capabilities.

(4) Advanced technology increases the automation of operational processes and functions and this poses a difficult challenge regarding technology dependence and force structure requirements. Automation can best be expressed as a state of technological activity where human interaction is limited or completely removed. Automation combines software, sensors and systems to enable a complex sequence of operations to be performed in varied environments and situations. Automation provides an opportunity to reduce force structure requirements or to repurpose existing force structure to areas of prioritization. The challenge occurs when trying to achieve

balance between automated capabilities and force requirements. Enough personnel must be available to continue operations when technology fails, is corrupted, is destroyed, or when operating in a degraded IE.

(5) Advances in AI and machine learning impact policies regarding human in the loop. To better understand these two technologies, it is important to grasp their basic principles. AI is defined by the DOD as "the ability of machines to perform tasks that normally require human intelligence". Machine learning is described as a sub-field of AI "that is closely related to statistics and allows machines to learn from data." This learning is accomplished through the use of training datasets that produce an AI model. AI and machine learning are foundationally dependent upon algorithms. An algorithm is a set of instructions used by machines to make calculations or conduct problem-solving tasks. As AI and machine learning are hosted within cyberspace infrastructure (interconnected devices) this is achieved through the use of software. Machine learning depends on algorithms that learn from and make calculations based on information. These algorithms build reference models from information to execute the previously mentioned calculations or decisions. Both machine learning and AI attempt in some degree to mimic the cognitive processes of the human brain to provide machines the ability to undertake tasks and decision making with a similar level of human cognition while also providing a means of human direction or control.[7]

(a) Cyberspace and EW operations, in conjunction with AI and machine learning enhanced cyberspace infrastructure, make it possible to connect sensors directly to shooters independent of human control. Current Army sensor-to-shooter networks can best be described as sensor-to-human-to-shooter with this construct used to keep a human decision maker as the final arbiter regarding the use of lethal force. This process lengthens the time between target identification and target engagement and has the potential to hinder successful execution of MDO significantly.

(b) Certain adversaries will most likely be unencumbered by this kind of restraint as history indicates that any available advanced technologies will find its way to the battlefield regardless of that technology's original purpose. Army forces must deny, degrade, disrupt, or destroy adversary capability as it relates to the sensor-to-shooter link at increasing speed, while simultaneously defending against an adversary's ability to do the same to friendly sensor-to-shooter links. Given that the human element is the slowest point in the link, consideration must be given how best to adapt the current human in the loop policy.

(6) Success in the advanced technology environment will also be predicated on building an accessible, extensible joint persistent training environment (PTE) that replicates contested and congested spectrum and cyberspace to enable individual, collective training, mission rehearsals, modeling, and simulation with high degrees of precision in both wired and wireless contexts.

2-2. The threat

a. A cyberspace threat is any circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a system resulting in a loss of confidentiality, integrity, or availability of cyberspace infrastructure or the information available for exchange

[7] Joint Artificial Intelligence Center. *Understanding AI Technology*. Allen, Gregory. April 2020 https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf

within and through that infrastructure.[8] Cyberspace threats not only involve an action but also require actors (threat agents) to execute that action in order to exploit cyberspace weaknesses and generate denial effects that disrupt, degrade, destroy, or manipulate friendly use of information.

b. Threats manifest themselves in combinations of national governments, terrorists, organized crime groups, hacktivists, hackers, bot-network operators, foreign intelligence services, insiders, phishers, spammers, and spyware and malware authors. These threats (via cyberspace and the EMS) may have access to sophisticated technologies such as robots, unmanned vehicles (aerial and ground), and weapons of mass destruction. They will merge cyberspace and EW capabilities enabling them to operate from disparate locations. Threats may hide among the population in complex terrain to thwart the Army's conventional combat overmatch. These threats do not have to be complex or expensive to prove disruptive.

c. State and non-state actors invest in capabilities to protect their access to cyberspace and disrupt or deny access to others. Use of these capabilities has the potential to negate current Army combat power and technological overmatch. Less capable adversaries will also use a variety of improvised weapons and technologies such as global navigation satellite systems (GNSS) jammers including those affecting global positioning system and radio frequency weapons that utilize the EMS to exploit Army reliance on technology.

d. The Army will see an increase in the number of devices and sensors connected to its cyberspace infrastructure. Since every device presents a potential vulnerability, this trend represents an exponential growth of targets through which an adversary could access Army cyberspace infrastructure, systems, and information. Conversely, the proliferation of devices presents opportunities for the enhanced synchronization of Army technologies and information to exploit adversary dependencies on cyberspace and the EMS.

e. An accessible and contested cyberspace domain and EME exacerbates the uncertainty of future conflict. More adversaries will gain access to cyberspace and EMS capabilities enabling them to fight across multiple domains and environments simultaneously. Adversaries will conduct complex cyberspace and EW attacks integrated with military operations or independent of traditional military operations. Difficult and untimely attribution of attacks in cyberspace, as well as the legal ambiguities of attacks in cyberspace, will complicate response actions.

f. Adversaries conduct sophisticated IW operations that leverage cyberspace and the EMS as a force multiplier across the IE. They use propaganda and disinformation through social media to affect public perception, sway public opinion that catalyze protests and violence in ways, and at a speed, that popular movements once took months or years to build. Cyberspace also provides adversaries an effective and inexpensive means for recruitment, propaganda, training, and C2.

g. The increased use of autonomous devices on the battlefield, including unmanned aerial systems provides challenges to security. The enhanced development of autonomous technologies portends a future where machines make some decisions for themselves on the battlefield using machine learning and AI. Consequently, these decision-making systems may be compromised and AI corrupted, posing a danger to Army forces and critical technologies. Because of the

[8] Joint Publication 3-12 U.S. Department of Defense, *Cyberspace Operations* (Washington, DC: United States Department of Defense, 2018)

proliferation of autonomous systems, fail-safe technologies and software are required to maintain positive control. This necessitates striking a balance between autonomous machines, advanced technology applications, human control, and staff support.

h. Advanced persistent threats (APT) or sophisticated cyberspace threats attempt to gain access to target networks and operate undetected to collect information or preposition exploits. An APT threat conducts OCO, gains access to a target network, and operates undetected (sometimes for a long period). To maintain access without discovery, the attacker must continuously rewrite code and employ sophisticated evasion techniques. The goal of some APTs or sophisticated cyberspace threats is to conduct a raid to exfiltrate data, recon the network and systems to determine key cyber terrain, and/or manipulate and destroy data. Additionally, other APTs seek to cause disruptions in the information environment or cognitive domain and are focused on employing cyberspace capabilities focused on causing physical destruction.

i. Threats to the EMS affect the Army in all operational environments. Peer and near-peer adversary threats are the most crippling and difficult to attribute. However, U.S. adversaries are not always responsible for EMS attacks. Insider threats and spectrum fratricide are as effective in denying Army use of the EMS, and in some cases, more of a detriment to operations.

Chapter 3
The Problem

3-1. Military problem
How does the Army, in conjunction with unified action partners, provide critical cyberspace and EW capabilities, to support MDO, while simultaneously denying the same to adversaries?

3-2. Central idea
Army forces, as part of the Joint force, conduct cyberspace and EW operations in an integrated and synchronized manner to create and exploit windows of superiority within or across multiple domains, the EMS, and the IE to seize, retain, and exploit the initiative to defeat the enemy.

3-3. Solution synopsis

a. MDO identifies three tenets that are required for Army forces to successfully execute operations: calibrated force posture, multi-domain formations, and convergence. The basic tenets of MDO are not new, what is new is the application of advanced technology that greatly compresses the speed of the decision cycle and creates the potential for increasing technology dependence on the part of Army forces. MDO is an information-centric and technology-dependent concept that relies on both attributes to enable a smaller geographically challenged force to engage with and defeat a larger more geographically secure force.

(1) From a cyberspace and EW perspective, enabling the three tenets of MDO is focused on supporting the speed of the decision-making cycle and the integration of advanced technology capabilities in a balanced manner, allowing the force to continue to operate during periods of technology failure, or when conducting operations in a degraded IE. This focus provides opportunities to address the capability of Army forces to challenge an adversary's ability to sustain

the speed of their decision-making cycle and the maintenance of their advanced technology integration.

(2) The rapid pace of technology deployment and the continual cyclic evolution of these capabilities directly impacts military operations. The application of advanced technology to military operations continues to compress the speed of the decision cycle and creates challenges in obtaining and maintaining a balance between human and automated processes and task execution. To support this data focused and technologically advanced environment cyberspace and EW operations place a greater emphasis on alignment to an operationally focused informational framework that generates effects based on cyberspace and EW capabilities. Cyberspace and EW operations and capabilities also provide integration and synchronization support to achieve combined effects within, and across multiple domains, the EMS, and the IE.

b. MDO requires calibrated force posture, multi-domain formations, and convergence to be executed successfully. None of these can be achieved without accurate, secure, timely, and sustained information available where and when needed. The quality, efficiency of use, and effective application of information is a critical aspect to the success of MDO. Scalable cyberspace and EW formations, equipped with tailored capabilities and infrastructure, conduct cyberspace and EW operations in support of MDO to provide targeted effects within and across all domains, the EMS and information space.

c. Solving the overarching military problem requires Army forces to understand five basic guidelines of cyberspace and EW operations.

(1) The primary use of cyberspace and the EMS is to facilitate the exchange of information. The primary purpose of operations within cyberspace and the EMS, to include EW, is to enable friendly information exchange while denying adversaries the same. Networks were conceived originally to exchange information. The Advanced Research Projects Agency (ARPA), the predecessor of the Defense Advanced Research Projects Agency (DARPA), pioneered the development of a network that could exchange information between research institutions. That original network eventually led to creation of the Internet. This fundamental focus on exchanging information has not changed. The vast majority of cyberspace and EW operations are concerned with enabling, defending, and supporting the ability to exchange information.

(2) Cyberspace and EW are IRCs. While cyberspace operations and EW are the key technical enablers of the integration and synchronization of IRCs, they are also IRCs themselves. This technically enabling aspect coupled with their informational nature increases the risk and vulnerabilities that each represent. Cyberspace and the EMS are used or accessed primarily as transmission mediums. EW is also primarily focused on maintaining friendly access to the EMS and denying the same to adversaries. Though cyberspace, EW, and the EMS have operational aspects not associated with the transmission of information, at their root these capabilities' major technological underpinnings are designed to support information transmission.

(3) Cyberspace and EW are the primary technical enablers of OIE. The Army is more dependent upon cyberspace, EW, and the EMS to conduct operations than other mediums or capabilities of information exchange.

(4) Cyberspace and EW operations will often be conducted in a degraded or denied EME and IE. Physical degradation of cyberspace infrastructure (including the EMS) may occur through a combination of configuration problems, environmental causes, or adversary activity directed against friendly cyberspace infrastructure that results in a degraded IE. Additionally, adversary directed disinformation campaigns and deception may be responsible for the cognitive degradation of the IE.

(5) All cyberspace operations are predicated on access and physics is an unrelenting constraint. Much, if not all, of the technical complexity and transmission constraints that exist within cyberspace and the EMS are grounded in the inter-relationships between physical properties conveyed over time, space, and scale that are expressed through the laws of physics. Bandwidth and EMS frequencies are finite resources with diminishing returns, network dependency, and geospatial limitations for every actor within the IE. To produce effects in support of MDO, cyberspace and EW forces must establish and maintain access to friendly and adversary cyberspace infrastructure including the EMS.

3-4. Components of the solution

Cyberspace and EW operations addresses support to MDO through three primary solutions: integrated cyberspace and EW capabilities, scalable cyberspace and EW formations, and cyberspace infrastructure.

a. Integrated cyberspace and EW capabilities.

(1) Cyberspace and EW integrated capabilities directly support the speed of the decision-making cycle by enhancing friendly information exchange while inhibiting adversary information exchange. To support friendly information exchange, the Army depends on an integrated communications architecture that connects strategic, operational, and tactical commanders across the globe. When directing integrated information, cyberspace, and EW capabilities against adversary capabilities, Army forces can search for, intercept, identify, characterize, locate, and target these systems to deliver both lethal and non-lethal effects that deny, degrade, or disrupt the adversary's use of cyberspace, the EMS, and the IE.

(2) Fully integrated cyberspace and EW operations provide organic capabilities to support Army forces, including formations engaged in independent operations, while also providing pooled capabilities that can offer remote support and augmentation as required. These capabilities integrate into force structure models and enable supported organizations to conduct all aspects of cyberspace and EW operations while providing support for integrating and synchronizing all warfighting capabilities in the execution of MDO. To maintain a military-technological edge and to prevail in MDO, the Army must continually evolve, adapt, and innovate. Cyberspace and EW technical capabilities incorporate automation, AI, and machine learning to enable cross-domain fires and cross-domain maneuver producing cross-domain synergy.[9]

(3) The generation of effects and the integration and synchronization support that cyberspace and EW operations provide are contingent upon the following processes and capabilities.

[9] TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-domain Operations 2028*

b. Cyberspace operations capabilities.

(1) OCO project power by applying force in and through cyberspace to deny and manipulate the adversary's access to the cyberspace domain. OCO rely on a systematic process to target and engage an adversary to create desired effects known as a kill chain. The Army's targeting doctrine defines the steps of this process as finding adversary targets that are suitable, fixing their location, tracking and observing, targeting with suitable weapons or assets to create desired effects, engaging the adversary, and assessing the effects generated. This is an integrated, end-to-end process described as a chain because any one deficiency interrupts the entire process.

(a) Effective OCO address the EMS, communications networks, information, information services, and associated cyberspace infrastructure. Offensive operations include cyberspace attacks, electromagnetic attacks, and physical attack against infrastructure and electromagnetics as well as exploitation type activities against cyberspace infrastructure. Offensive operations are predicated on access, which means there is an opportunity and technical capability to gain exposure to, connectivity to, or entry into a device, system, or network to enable further operations.

(b) In some cases, accesses can be created remotely with or without permission of the infrastructure's owner. In other situations, access to closed networks or virtually isolated systems may require physical proximity or more complex and time-consuming processes.

(2) DCO consist of activities to protect against, detect, characterize, counter, and mitigate cyberspace threat events generated by adversary cyberspace operations. DCO defends cyberspace infrastructure to preserve information exchange. DCO passively and actively preserve the ability to utilize friendly force cyberspace capabilities while protecting data, networks, and other designated systems. Cyberspace and EW operations facilitate freedom of action in the EMS by offering capabilities that reprogram wireless network systems in response to validated changes in equipment, tactics, or the EME. Cyberspace and EW operations can additionally deceive the adversary by deliberately radiating, re-radiating, altering, suppressing, absorbing, denying, enhancing, or reflecting electromagnetic energy from wireless systems in a manner intended to convey misleading information to an adversary. These operations also include countermeasures consisting of devices and techniques, threats, and tactics, techniques, and procedures that employ wireless technology to impair the effectiveness of adversary activity.

(3) Defensive cyberspace operations-response actions (DCO-RA) are operations that are part of a DCO mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. Because the actions occur outside of the DODIN-A, DCO-RA are subject to legal constraints and restraints. DCO-RA require authorization according to standing and supplemental rules of engagement.

(4) Defense Cyber Operation- Internal Defensive Measures (DCO-IDM) are operations in which authorized defense actions occur within the defended portion of cyberspace. Most DCO missions are DCO-IDM, which include pro-active and aggressive internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses used to eliminate these threats and mitigate their effects. DCO-IDM activities are responses to

unauthorized activity, alerts, or threat information within the defended network that leverage intelligence, counterintelligence, law enforcement, and other military capabilities, as required.

(5) DODIN operations consist of actions taken to secure, configure, operate, extend, maintain, and sustain cyberspace infrastructure in a way that creates and preserves the confidentiality, availability, and integrity of the DODIN-A. The DODIN-A, and its underlying cyberspace infrastructure, is the baseline information exchange platform for Army operations. DODIN operations include proactive measures such as configuration control, patching, information assurance measures, physical security, secure architecture design, operation of host-based security systems and firewalls, and encryption of data. The DODIN-A as the foundation of cyberspace infrastructure serves as the primary enabler for OIE.

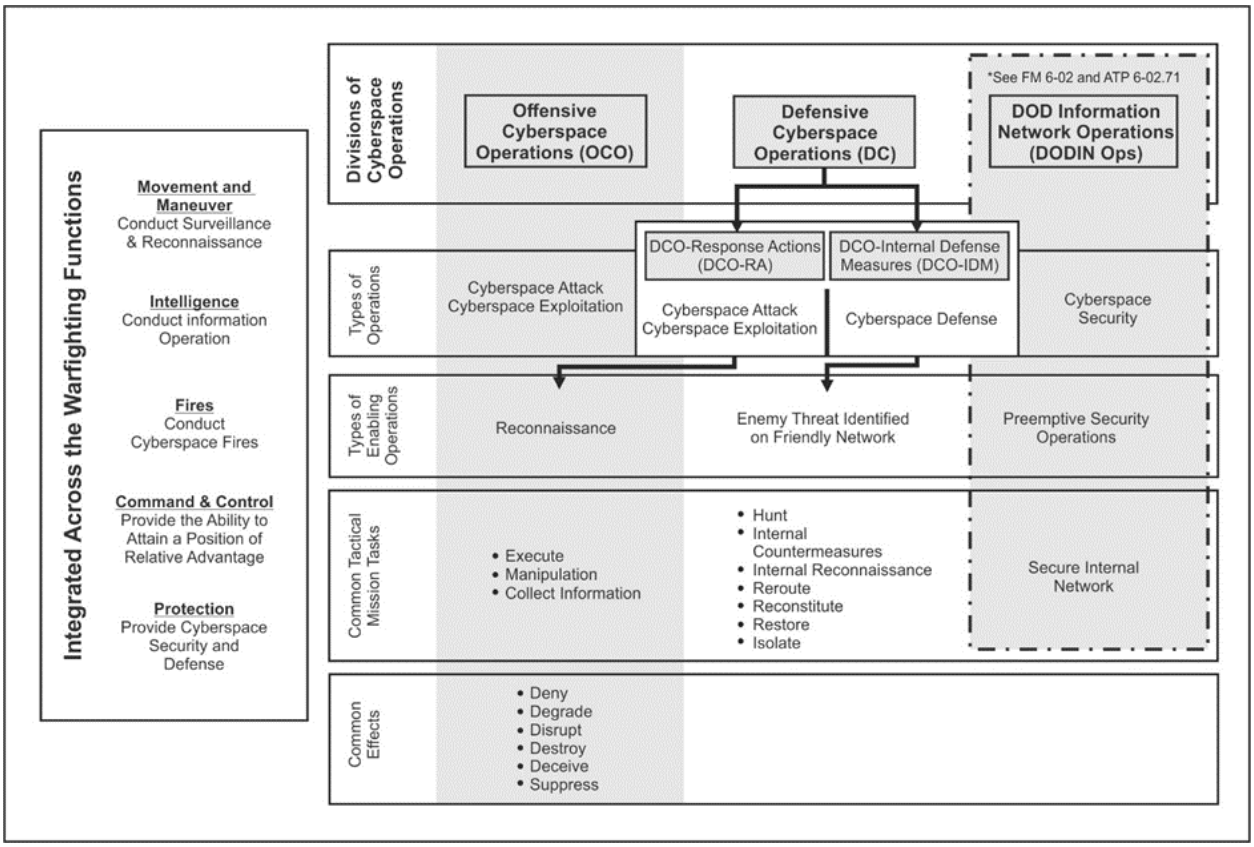


Figure 3-1. Integrated Cyberspace Operations Capabilities

c. EW operations capabilities. EW is any military action involving the use of electromagnetic or directed energy to control the EMS or to attack the enemy. EW consists of three subcomponents: Electromagnetic Attack (EA), Electromagnetic EP), and Electromagnetic Support (ES). Cyberspace and EW are mutually supporting and seek to preserve the use of cyberspace infrastructure and the IE. The following describes these subcomponents.

(1) EA is a subcomponent of EW where actions are taken to prevent or reduce the adversary's effective use of the EMS. These actions include but are not limited to jamming and electromagnetic deception. EA uses electromagnetic energy, directed energy, and anti-radiation

weapons to attack radio frequency capabilities tied to personnel, facilities or equipment with the intent of degrading, neutralizing, or destroying the adversary's combat capability.

(2) EP refers to actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, or adversary use of the EMS, as well as some naturally occurring phenomena that degrade, neutralize, or destroy Army combat capability. EP facilitates cyberspace infrastructure defense through electromagnetic (EM) hardening (which filters, attenuates, grounds, bonds, blanks, and shields against undesirable EM effects), EM interference resolution (which systematically diagnoses the cause or source of the interference), and EMS control and electromagnetics security (which are measures designed to deny unauthorized persons information).

(3) ES involves actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conducting future operations. ES enables Army forces to identify the electromagnetic vulnerability of an adversary's electromagnetic equipment and systems. ES systems collect data and produce information as well as corroborate other sources of information or intelligence, conduct or direct EA operations, create or update EW databases, initiate self-protection measures, support EP efforts, support IRCs, and target enemy or adversary systems.

(4) ES and signals intelligence (SIGINT) missions may use the same or similar resources. The two differ in the intent, purpose for the task, the detected information's intended use, the degree of analytical effort expended, the detail of information provided, and the timelines required. ES missions respond to the immediate requirements of a tactical commander or to develop information to support future cyberspace or EW operations. However, the SIGINT components of electromagnetic intelligence (ELINT), communications intelligence (COMINT), and foreign instrumentation signals intelligence (FISINT) provide the library by which EW/ES systems operate. Ensuring the effective integration of SIGINT, EW, and cyberspace operations capabilities is one of the most complex aspects of integrating and synchronizing cyberspace and EW operations with other functions. Effective integration extends well beyond simple coordination. SIGINT, EW, and cyberspace operations occur completely or partially within the same portion of the EMS and share many interrelated considerations.

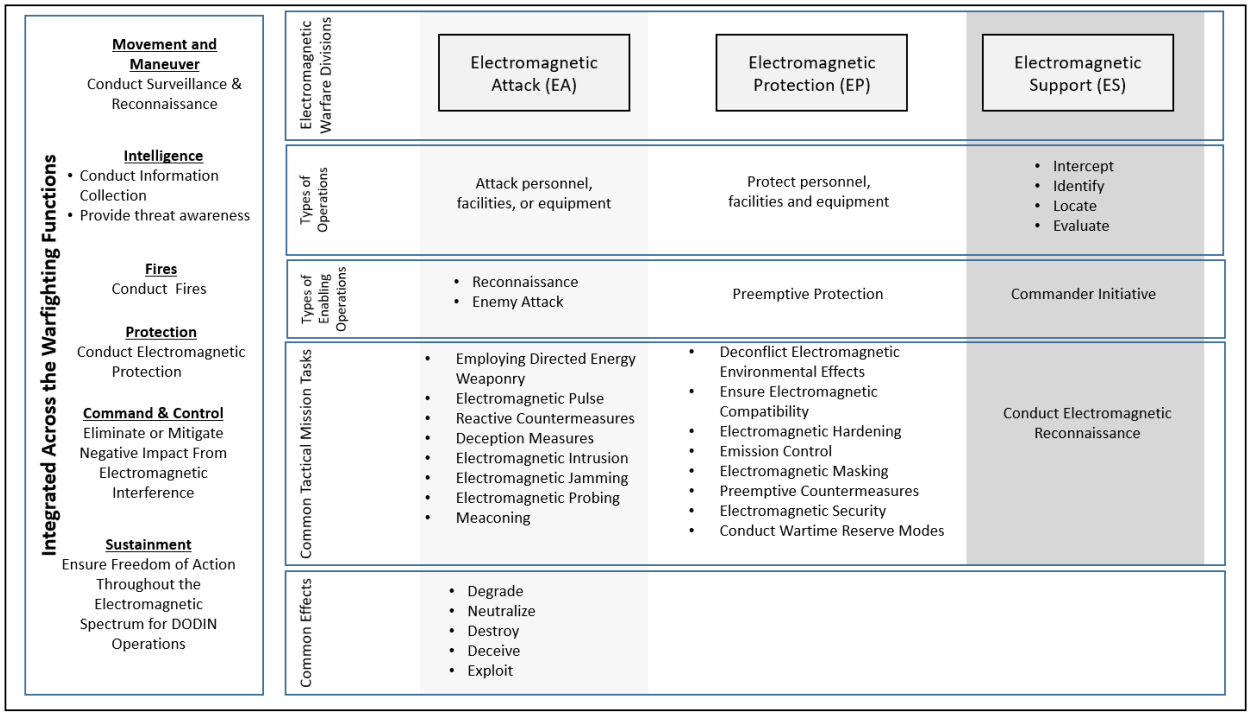


Figure 3-2. Integrated Electromagnetic Warfare Operations Capabilities

(5) Effective integration requires de-conflicting and identifying windows of opportunity between EA, EP, and ES functions. Therefore, integrating SIGINT, EW, and cyberspace operations requires close staff collaboration, detailed procedural controls, and the use of technical channels. The following includes some of the interrelated aspects of these four functions:

- Planning, tasking and cross-cueing between functions.
- Conducting collection and re-tasking assets.
- Using technical channels.
- Allocating assets and bandwidth.
- Understanding and applying intelligence gain/loss (IGL) assessments.

d. Supporting capabilities.

(1) Intelligence, surveillance, and reconnaissance (ISR) include activities in cyberspace and the EME to gather intelligence from target and adversary systems that may be required to support future operations. ISR contributes directly to cyberspace situational understanding as it enables the commander to defend the network, target threats, and integrate early warning concurrently to manage risk. ISR applies to an adversary as well who must gather intelligence within the Army's portion of the DODIN continuously to execute their own offensive operations effectively.

(2) Intelligence preparation of the battlefield (IPB) to support cyberspace and EW operations consists of predictive analysis used along with intelligence and non-intelligence enabling activities, conducted to plan and prepare for potential follow-on military operations. Army cyberspace and EW forces use IPB to gain and maintain access to systems and processes, and to position capabilities to facilitate follow-on actions. IPB includes identifying data, software, system

and network configurations, or physical structures connected to, or associated with, the cyberspace infrastructure for determining system vulnerabilities. Additionally, IPB includes actions taken to assure future access and/or control of the system, infrastructure, or data during anticipated hostilities. IPB and civil preparation of the battlefield (CPB) products are key inputs for the IPB. As part of IPB, ARSOF provides cyberspace forces with the physical access needed through its placement in the deep fires area.

(3) Situational understanding (SU) is the requisite current and predictive knowledge of the OE, IE, EME, and cyberspace domain upon which operations depend, including all factors affecting friendly and adversary cyberspace forces. Improved SU enables informed decision making at all levels via flexible and focused products and processes.

(4) Successful integration and synchronization of cyberspace and EW capabilities is predicated on building an accessible, extensible PTE that replicates contested spectrum and cyberspace to enable individual and collective training, modeling and simulation, and mission rehearsals, with a high degree of precision in both wired and wireless contexts. This will require the ability to emulate the cyberspace and EMS portions of the IE.

e. Integrated support to OIE.

(1) Conducting integrated support to OIE. The Army counters adversary cyberspace and EW threats, mitigates a degraded IE, and takes actions against enemy cyberspace and EW capabilities to support OIE. Army forces detect and disrupt adversaries' cyberspace and EMS enabled operations while performing emissions control and other means of signature management effectively. Communications systems provide external connectivity to global support networks however, units are not dependent on continuous connectivity to fight as Army forces possess the ability to operate within a degraded or denied IE.

(2) Cyberspace and EW operations provide capabilities that enhance the impact to potential adversaries in the cognitive, physical, and informational dimensions creating multiple dilemmas. Cyberspace and EW are the primary technical enablers of the integration and synchronization of IRCs to support OIE. OIE are conducted to support a commander's information strategy which in turn is aligned to a broader more comprehensive information strategy.

f. Scalable cyberspace and EW formations.

(1) The Army provides strong and resilient cyberspace and EW forces capable of supporting operational demands through technologies that minimize bandwidth constraints, centralize computing operations in a common operating environment, and standardize the provisioning of network services across the Army. Cyberspace and EW operations can be executed from anywhere provisioned with cyberspace infrastructure that provides access to the cyberspace domain and the EMS. This ensures that cyberspace and EW forces need not be present within a designated operational area to deliver effects.

(2) Scalable cyberspace and EW formations provide organic capabilities to support maneuver forces including those engaged in independent operations, while also providing pooled capabilities

that can offer remote support and augmentation to all multi-domain formations. These scalable formations integrate into existing force structure models and enable supported organizations to conduct all aspects of cyberspace and EW operations. Globally tailored cyberspace mission forces enhance a commander's ability to maneuver by creating denial effects from home station or close to the fight.

(3) Scalable cyberspace and EW formations enable multi-domain formations to achieve convergence of all capabilities to achieve a position of advantage across all domains, the EMS, and the IE. Army forces use cyberspace capabilities to exploit psychological, technological, temporal and spatial advantages over the adversary. This requires understanding the local effects that cyberspace and EW operations produce while also understanding the potential effects that could be produced far beyond the local focus of operations. It also requires understanding that cyberspace and EW effects can be generated from strategic distance and still produce local effects. This is accomplished by generating and applying both organic and remote cyberspace and EW capabilities to support Army forces in exploiting enemy vulnerabilities, seizing and retaining key terrain, to include key terrain in cyberspace, and holding targets at risk for sustainable outcomes. Cyberspace and EW capabilities integrate fully into the targeting process, facilitating synchronization and integration of multiple elements of combat power to gain an advantage, protect that advantage, and place adversaries at a disadvantage.

(4) Scalable cyberspace and EW force structure provide organizations with balanced combinations of capacity, capability, and position, with the ability to maneuver across strategic, operational, and tactical distances. Scalable cyberspace and EW force structure includes:

(a) Forward presence forces. Forward presence forces consist of Army forces operating locally in forward positions around the world. Cyberspace and EW forward presence forces include organizations with a wide array of capabilities providing timely and sustained support to MDO. These forces provide enhanced interoperability with partners, proxies, and surrogates through integration into existing operational and support structures that are difficult for expeditionary forces to establish in a crisis or conflict. The persistence of these forward presence forces is a foundational element of the dynamic employment of cyberspace and EW capabilities as it enables strategic, operational, and tactical maneuver across all domains with the full integration and synchronization of other warfighting capabilities.

(b) Multifunctional formations. Multifunctional formations that include cyberspace and EW capabilities possess the combination of capacity, capability, and endurance which generates the flexibility necessary to execute MDO. All Army cyberspace and EW formations are multifunctional to some degree. Multifunctional formations conduct cyberspace and EW operations across all domains and the IE. The most important materiel contributors to flexibility are advanced cyberspace infrastructure, platforms, and payloads.

(c) Expeditionary forces. Expeditionary cyberspace and EW forces are those formations ready to maneuver both physically, and virtually from reach-back across strategic distances, while in contact with the adversary's capabilities. Cyberspace and EW forces that deploy physically bring their equipment or draw prepositioned equipment and are ready to fight within days or a few weeks of alert. Expeditionary forces deploying by sea are ready to fight within weeks.

Expeditionary forces may have to conduct joint forcible entry operations in the absence of forward presence forces or to open an additional line of operation. In conflict, the speed and effectiveness with which expeditionary forces can deploy along contested lines of support and communications is decisive to successful execution of MDO.

(d) National-level capabilities. National-level capabilities include cyberspace and EW capabilities normally controlled above the theater level. These capabilities complement forward presence and expeditionary forces with their unique effects, global reach, and rapid execution that require little or no physical movement. The scarcity of these resources and the potential for unintended consequences with their use might cause policymakers to retain authorities or permissions for their use. The extensive preparation required to use these resources must begin in competition when U.S. forces develop detailed intelligence identifying specific vulnerabilities, gain or prepare to request required authorities, and train to use national-level capabilities.

(5) Authorities. The Army uses the appropriate policy and authorities to coordinate with other agencies to conduct actions in and through cyberspace the EMS, and the IE.

(a) Many of the effects generated by cyberspace and EW operations require considerable legal and policy review. This is also true of effects designed to support OIE. This review often creates lengthy lead times during the planning and preparation, even though the effects may occur nearly instantaneously once executed. Delegating authority under pre-established rules of engagement lessens the time and complexity in developing and applying cyberspace and EW effects.

(b) The Army possesses clear authorities and policies to deter, prevent, detect, defend against, respond to, and remediate hostile actions in cyberspace, the EMS, and the IE. The authorities and rules of engagement for cyberspace and EW operations will continue to evolve, this evolution continues to accelerate as the understanding of the cyberspace domain, the EMS, and the IE continues to mature.

(c) Authority for actions undertaken by the Army are derived from the U.S. Constitution and Federal law. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace and EW. Key statutory authorities that apply to the Army include Title 10, USC, Armed Forces; Title 18, USC, Crime and Criminal Procedure; Title 32, USC, National Guard; Title 40, USC, Public Buildings, Property, and Works; Title 44, USC, Public Printing and Document; and Title 50, USC, War and National Defense. Conducting cyberspace and EW operations may involve directives stemming from any combination of these authorities. (See Appendix G for more information regarding authorities).

g. Cyberspace infrastructure.

(1) In modern competition and conflict, cyberspace infrastructure and the information it modifies, stores, protects, and exchanges have become as important as lethal action in determining the outcome of operations. Across all warfighting and supporting functions and their related capabilities there has been an overemphasis on system related solutions to information focused

challenges. Development of system-oriented solutions is often undertaken with little regard to interoperability or the integration and synchronization requirements of cyberspace infrastructure support and security. Separating information requirements from the physical infrastructure is critical to successfully orienting the Army toward the demands of an information-centric operating environment.

(a) Cyberspace infrastructure is network agnostic as it supports all users. From intelligence to fire control to aviation, all networks of purpose defined by the information to be exchanged can simultaneously coexist within the framework of cyberspace infrastructure. In today's world this is sometimes challenging but in a future with more prevalent semi-independent and independent information-centric technologies like AI, machine learning, and autonomous systems, network connections will be ad hoc and information exchange and interconnectivity will fluctuate at speeds beyond human abilities to manage and control.

(b) Machine learning, AI, and their software will reside in autonomous devices that are part of cyberspace infrastructure. The purposes and functions of these technologies will be varied as will the networks of purpose they support (Fires, intelligence, and others), differentiating the infrastructure from the network of purpose as defined by the information to be exchanged is important to the effective application of these technologies to military operations. This will make convergence of capabilities easier as the focus will be on the information exchange required to achieve convergence and less on the infrastructure required to complete that information exchange.

(2) Cyberspace infrastructure is identified as a combination of manmade and naturally occurring mediums, including portions of the EMS, over which information is created, collected, processed, stored, and transmitted. Any device or system designed to exchange information through wired or wireless connectivity is a component of cyberspace infrastructure. Emphasis is placed on the purpose, type, format, volume, and time sensitivity requirements of the information to be exchanged so that infrastructure design and support can be devised regardless of warfighting function or capability. In many cases information can be exchanged across a common platform and separated by function, purpose, or capability through software manipulation. The Army develops and deploys cyberspace infrastructure through adherence to a common operating environment (COE). The COE is an Army standard for cyberspace infrastructure development that is divided into six computing environments (CEs): Command Post (CP), Mounted, Mobile/Handheld, Data Center/Cloud/Generating Force, Sensor, and Real-Time/Safety Critical/Embedded CEs. CEs are not mutually exclusive but instead work together and share the standards-based substructure to drive operational costs down. The COE identifies cross-cutting capabilities used by many systems, such as geospatial visualization and secure authentication, and delivers a common software baseline employed by all of the CEs.

3-5. The EMS as a component of cyberspace infrastructure

a. Cyberspace and the EMS have a profound synergy both technically and operationally. EMS links and wireless infrastructure are components of the physical layer of cyberspace.[10] Cyberspace and EW operations therefore involve the use of the EMS, wireless communication technologies, and systems that enable all warfighting and supporting functions. Because EMS links and wireless

[10] Joint Publication 3-12 U.S. Department of Defense, *Cyberspace Operations* (Washington, DC: United States Department of Defense, 2018)

infrastructure comprise part of the physical layer of cyberspace, portions of the EMS are considered a primary component of cyberspace infrastructure that spans a specific range of frequencies (spectrum) of electromagnetic radiation and their respective wavelengths and photon energies.

b. The ability to integrate and direct EMS-enabled assets at all levels of command is critical to effective MDO execution. Army forces use cyberspace and EW capabilities to plan and manage use of the EMS to combat the strengths, while exploiting the vulnerabilities, of an evolving range of adversary capabilities. Use of EMS and EMS-enabled capabilities to achieve effects reduces risk by limiting the exposure of combatants and presents commanders with an array of nonlethal options that achieve effects unattainable through lethal means. When using EMS and EMS-enabled assets, consideration must be given to signature management and reduced signature footprint. These actions deny opponents an actual or perceived advantage in the EMS and support freedom of maneuver within the IE.

3-6. Integrating functions

a. Enable cross-domain maneuver. Cyberspace and EW operations enable force projection without the need to establish a physical presence. Maneuver in cyberspace and the IE includes such actions as gaining access to adversary, enemy, or intermediary links and nodes and shaping cyberspace and the IE to support future actions. Maneuver in cyberspace and the IE is supported foundationally through the movement of information. These actions produce cascading effects that ensure Army forces maintain the ability to maneuver within, and across all domains, the EME, and the IE. When planned and executed in concert with Army Special Operations Forces (ARSOF); the application of cyberspace and EW operations presents multiple dilemmas for the adversary and prompts the redirecting of enemy resources to respond accordingly.

b. Enable cross-domain fires. Army cyberspace and EW operations provide integration and synchronization of cyberspace and EW into the intelligence, planning, and targeting processes to achieve required effects. Cyberspace and EW enabled cross-domain and counter-fire sensors improve commander’s situational understanding and support suppression or destruction of enemy fires systems, enabling commanders to seize opportunities and produce cyberspace and EW effects at the time and place of their choosing to achieve localized effects by extending cyberspace capabilities to the tactical edge.

c. Enable cross-domain synergy. The Army conducts cyberspace and EW operations to retain freedom of movement within the cyberspace domain, the EME, and the IE. Cyberspace and EW operations enhance operations across all domains and environments through the creation of singular and combined effects achieved through integration and synchronization of warfighting capabilities and IRCs. Cyberspace and EW operations enable the movement of information to a place or process where it has maximum military utility. The Army uses cyberspace and EW operations to exploit emerging technical capabilities, including persistent systems that can generate, capture, reconfigure, store, and disseminate information that feeds advanced analytic processes that provide accelerated decision-making support.

Chapter 4
Conclusion

a. The future OE drives the need for significant change and improvement in how the Army uses and protects its current, planned and forecasted cyberspace, EW, and other information-related capabilities. Establishing support to MDO under the three areas of integrated cyberspace and EW capabilities, scalable cyberspace formations, and cyberspace infrastructure requires enhancement of the Army's approach to managing its cyberspace, EW, and information infrastructure, content, and effects.

b. This concept identifies the capabilities needed to provide integrated and synchronized cyberspace and EW operations that serve as the foundation for converging warfighting and supporting capabilities in support of MDO. This document also provides a pathway for development of an institutional foundation for cyberspace and EW operations that results in resilient, protected, multi-tiered, and rapidly configurable cyberspace infrastructure. This document also outlines adaptable, scalable, and technically robust EW capabilities that when integrated and synchronized with cyberspace capabilities produce windows of superiority that enhance information advantage in support of MDO. This cyberspace and EW foundation establishes and enables an information advantage in support of MDO while being responsive to the needs of the commander's decision cycle in all operational environments.

Appendix A
References

Army doctrinal publications are available online: https://armypubs.army.mil.

Joint publications are available online: https://www.jcs.mil/doctrine.

Section I
Required References

TRADOC Pamphlet 525-3-1
The U.S. Army in Multi-domain Operations 2028

Section II
Related References

Army Doctrine Publication 2-0, *Intelligence*. 31 July 2019

Army Doctrine Publication 3-0, *Operations.* 31 July 2019

Army Doctrine Publication 5-0, *The Operations Process.* 31 July 2019

Army Doctrine Publication 6-0. *Mission Command: Command and Control of Army Forces.* 31 July 2019

Army Techniques Publication 2-01.3, *Intelligence Preparation of the Battlefield*. 1 March 2019

Army Techniques Publication 3-12.3, *Electronic Warfare Techniques.* 16 July 2019

Joint Publication 2-0
U.S. Department of Defense *Joint Intelligence.* (Washington DC: United States Department of Defense, 22 October 2013)

Joint Publication 3-0
U.S. Department of Defense *Joint Operations*. (Washington DC: United States Department of Defense, 17 January 2017 w/Change 1 dated 22 October 2018)

Joint Publication 3-12
U.S. Department of Defense, *Cyberspace Operations* (Washington, DC: United States Department of Defense, 2018)

Joint Publication 3-13.1
U.S. Department of Defense *Information Operations* (Washington, DC: United States Department of Defense, 2012 w\Change 1 2014)

Joint Publication 3-85
U.S. Department of Defense *Joint Electromagnetic Spectrum Operations* (Washington DC: United States Department of Defense, 22 May 2020)

Joint Publication 5-0
U.S. Department of Defense *Joint Planning* (Washington DC: United States Department of Defense, 16 June 2017)

Joint Publication 6-0
U.S. Department of Defense *Joint Communications System* (Washington DC: United States Department of Defense, 10 June 2015)

Understanding AI Technology. Joint Artificial Intelligence Center. Allen, Gregory. April 2020

U.S. Army Field Manual 3-12
Cyberspace and Electromagnetic Warfare Operations. April 2017

U.S Army Field Manual 3-13
Information Operations. 6 December 2016.

U.S Army Field Manual 6-02
Signal Support to Operations. 13 September 2019.

Appendix B
Required Capabilities

B-1. Introduction

a. The Army's ability to leverage cyberspace and EW capabilities is critical to its operational success. Cyberspace and EW capabilities will integrate fully with other capabilities and provide integration and synchronization support to all capabilities at the commander's disposal to gain advantage, protect that advantage, and place adversaries at a disadvantage.

b. Cyberspace and EW operations support to MDO requires a sustained path for capability development into the future. The following required capabilities are essential to establishing this path to the future.

B-2. Required capabilities

a. Army forces require the capability to synchronize and assess OCO to attack enemy and adversary facilities, platforms, sensors, systems, networks, critical infrastructure, key resources, and information to deny, degrade, disrupt, destroy, or manipulate enemy and adversary capabilities and actions to gain and maintain friendly freedom of action, ensure friendly C2 while denying the same to enemies and adversaries during MDO. (3-4 b(1), b(1)(a))

b. Army forces require the capability to conduct defensive cyberspace operations, response actions and internal defensive measures, to secure, detect, mitigate, and remediate cyber incidents to support MDO. (3-4 (2), (3), (4))

c. Army forces require the capability to provide the commander situational understanding of cyberspace and the EMS of adversary (foreign and insider), friendly and neutral capabilities, plans, intentions, and actions on networks, services and systems, the potential impact(s) on the mission and force, how to mitigate and respond to those adversary actions, as a part of cyber-security, DCO and OCO, while supporting MDO. (3-4 d (1), (2), (3))

d. Army forces require the capability to emulate the cyberspace and EMS portions of the IE to support training and operations in support of MDO. (3-4 d. 4)

e. Army forces require the capability to engineer, construct, operate, and sustain an Army enterprise (architecture and tools) to support defensive and offensive cyberspace operations, situational understanding, emulations and their associated activities to support MDO. (3-4 b (5), 3-4 g (2) (a), (b))

f. Army forces require the capability to conduct legal, regulatory and policy analysis and coordination for cyberspace and EW operations to support timely decision making in MDO. (3-4 f (5) (a), (b), (c))

g. Army forces require the capabilities and authorities to collect, analyze, and exploit (site exploitation and forensics), information from or about enemy and adversary cyberspace and EMS

dependent facilities, platforms, sensors, systems and networks to gain and maintain friendly freedom of action, ensure friendly C2 while denying the same to adversaries during MDO. (3-4 d (1), (2))

h. Army forces require the capability to research, develop, engineer, acquire, and deploy solutions in a time-sensitive manner to enable effective cyberspace operations and associated activities to support MDO. (3-4 g (2) (c))

i. Army forces require the capability to perform threat-based security and vulnerability assessments for cyberspace and EW operations to support MDO. (2-2 a-i, 3-4 (2)-(4) (d) (2))

j. Army forces require the ability to conduct Electromagnetic attack to detect, deceive, disrupt, degrade, and destroy adversary use of the EMS to support MDO. (3-4 c (1)-(5))

k. Army forces require the ability to plan, coordinate, and integrate Electromagnetic warfare activities to support MDO. (3-4 c (1)-(5))

l. Army forces require the ability to protect personnel, platforms and systems against the effects of enemy, friendly, or neutral use of the EMS in support of MDO. (3-4 c (2))

m. Army forces require the ability to attack and exploit adversary personnel, platforms and systems to support MDO. (3-4 b (1) (a)-(b)), 3-4 c (1))

n. Army forces require the capability to utilize the EMS to conduct OCO to support MDO. (2-1 (3) (b), 3-4 b (1) (a)-(b))

o. Army forces require the capability to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy (Close Area to the strategic deep fires Area) for the purpose of immediate threat recognition, targeting, planning and conduct of future operations to support MDO. (3-4 c (1) - (5))

p. Army forces require the capability to plan and rapidly de-conflict and change frequencies used by friendly systems (communications, radar, EW, SIGINT, and others) in a congested and contested environment, to support MDO. (3-4 c (1)-(5))

q. Army forces require the capability to establish secure cyberspace infrastructure as a part of the joint and Army information enterprise, transmitting data at multiple levels of classification, to include partner classifications, to support MDO. (3-4 (2) - (5) (c) (1)-(5), 3-5 a-b)

r. Army forces require the capability to provide global, secure, adaptive and rapid access to the DODIN with trusted and authenticated domains, at multiple levels of classification to all authorized entities requesting interaction with resources from any location, at any time, to support MDO. (2-2 a-I, 2-4 b (5))

s. Army forces require the capability to integrate with MDO partner cyberspace infrastructure securely during garrison and deployed operations, including those partner networks with different intelligence sharing relationships, to enable MDO. (3-4 f (4) (a), Appendix D a-b)

t. Army forces require the capability to discover, deliver, and store data with multiple levels of classification securely, to include MDO partner classifications, to provide users with awareness of relevant, accurate information, and automated access to newly discovered or recurring information, for timely and efficient delivery in a usable format, to support MDO. (3-4 b (5))

u. Future Army forces require the capability to train and prepare leaders/soldiers on the skills and expertise required to analyze Cyber/EW threats; conduct Cyber/EW planning and threat mitigation and synchronize and converge Cyber/EW effects across the battlefield and competition continuum. (3-4 b (5))

v. Army forces require the ability to operate, maintain, protect, and rapidly restore disrupted portions of the communications network during competition, conflict, and the transition periods in between. (3-4 b., 3-5 c. 1-3)

Appendix C
Science and Technology

C-1. Introduction

a. The following represent science and technology (S&T) enablers providing adaptive capabilities that ensure the security of cyberspace infrastructure while increasing the overall capabilities of cyberspace and EW operations. The cyberspace and EW systems used by the Army to conduct MDO require investments in both foundational and advanced research. Building cyberspace and EW capabilities capable of reacting to current and future needs over a broad range of potential operations requires a delicate balance between the needs of today and those of the future. Achieving this balance begins with a clear understanding of the S&T landscape, especially the enabling and destabilizing role of emerging and disruptive technologies.

b. Integration of innovative technologies with cyberspace and EW operations will allow commanders to better understand the impact of their decisions, make adjustments to their plans, and successfully execute MDO. Focus on the identified technology investment areas listed below positions the Army for near-term transformation and builds a sustained path to future capability development that is crucial to the successful implementation of the MDO concept. Additionally, these technology investment areas are aligned to current Army modernization priorities.

c. These technology priorities also support efforts being undertaken as part of the Network Modernization Cross Functional Team (CFT). Future S&T priority documents may reflect technologies identified as promising within ongoing CFT activities.

C-2. Foundational research

a. Big data analytics. These technologies focus on data that presents significant volume, velocity, variety, veracity and visualization challenges. Increased digitalization, a proliferation of new sensors, new communication modes, the internet-of-things and virtualization of social communication have contributed significantly to the development of these technologies. Advanced data analytics concerns advanced processes and methods for understanding and visualizing large volumes of information. These techniques span a wide range of methods drawn from research areas across the data sciences, including AI, automation, modelling and simulation, and human dynamics engineering. These technologies enable increased operational efficiency, reduced costs, improved logistics, real-time monitoring of capabilities and predictive assessments of operational plans. These technologies also enhance situational understanding at the enterprise, strategic, and tactical levels. AI is the pivot around which big data will be turned into actionable knowledge and, ultimately, an information and decision advantage.

b. AI and machine learning. These technologies will assess and interpret vast amounts of sensor and intelligence data to produce actionable information and recommendations for the warfighter. These technologies have the capacity to make independent decisions and act upon these decisions rapidly, while at the same time, have the ability to work as part of a team which includes humans. AI and the subset of machine learning focus on algorithms that can learn from and make decisions based on data.

(1) These technologies are incorporated into systems design to provide semi or full autonomy based on standards, protocols, and technical sophistication. Many of these technologies will collaborate with humans who will retain control and final decision-making authority while enhancing situational understanding, operational reach, and reducing the risk to personnel during operations.

(2) Integration of AI and machine learning into operations will allow for rapid and more effective human and machine decision making. Use of AI and machine learning on sensors to pre-process information and provide adaptive use of frequencies (cognitive RF) and bandwidth leads to a decrease in communication traffic. Autonomous cyberspace infrastructure management and defense are key areas of focus for these technologies. AI and machine learning applications designed to support OCO and EA will be critical to executing MDO successfully. These technologies have the potential to impact the speed of the decision cycle decisively and enhance the targeting process significantly.

c. Integrated EW. As wired and wireless technology use has proliferated, the Army has become more dependent on these technologies. This dependence places enhanced emphasis on developing and operationalizing EW as an integrated battlefield capability that enhances situational awareness, improves force protection, enables dominant maneuver, and aids in precision lethality. Integrated EW technologies will provide an offset as potential adversaries' transition towards advanced EW threat techniques. These technologies will also support enhanced SMO. SMOs are the interrelated functions of managing EMS resources, frequency assignment, host nation coordination, and monitoring of spectrum management policy that together enable the planning, management, and execution of operations within the EME. Technologies supporting SMOs enhance convergence and cyberspace infrastructure management activities. These technologies will support a final goal to have Electromagnetic situational awareness system, which includes full

spectrum passive and active long-range multi-platform EM sensing, interactive data fusion, AI-enhanced analytics, and active EM/cyber response

d. Cyberspace SU. Cyberspace SU is developed through a family of interactive, interoperable, and critical technologies that facilitate maneuver planning, collaboration, and synchronization through integration with the commander's user-defined operational picture. Technology that supports this effort focus on capabilities to automatically incorporate data from multiple sources and automatically configure this data in multiple formats. This data resource should be easily maneuvered via sorting, filtering, etc. and should be amenable to visualization schemas that can be configured by users. This data needs to be configurable to be incorporated into models and analyzable through numerous processes and scientific techniques as required by the user. Cyberspace SU will be fielded within the Army's command post CE, establishing a framework to integrate fielded and emerging capabilities into operations.

(1) These technologies support capabilities to coalesce and investigate data to support intelligence reporting, influence analysis and public messaging strategies. Additionally, these capabilities will aide in developing network analysis, influence analysis "maps" and visualizations of information environment activities using data from multiple platforms, and the underlying models to enable situational understanding, uncover hidden relationships, and link cyberspace to operations.

(2) These technologies will generate multiple historical baseline instances of the cyberspace domain, the EME, and IE (capturing a 'complete' picture of these domains and environments at multiple intervals throughout time), with ability to show change between instances to use in live training. Historical baselines will enable analysis of the cyberspace domain and related environments leading up to known historical events to identify potential indicators, analysis across time to see how each respond to certain stimuli and allow all current and future predictive analytical capabilities to be tested through simulation and analysis.

e. Hardware and software convergence. Develop and implement hardware and software standards that enable collapsing multiple C2, intelligence, and EW systems and functions into a common chassis with synchronized and concurrent operation. This capability allows synchronized multiple use of antennas, reduces the amount of cabling and connections required, and generally reduces the size, weight, and power required for mounted and dismounted cyberspace operations.

f. Autonomous active cyberspace defense. Autonomy is the ability of a system to respond to situations by independently composing and selecting among different courses of action in order to accomplish goals based on knowledge and a contextual understanding of the world, itself, and the situation. Autonomous active cyber defense detects, evaluates, and responds before a human operator could understand and react. These technologies focus on systems which provide autonomous active cyberspace defense through a collection of synchronized, real-time capabilities to discover, define, analyze, and mitigate cyberspace threats and vulnerabilities without direct human intervention. These technologies include sensor-based AI that learns and manages network topologies, identifies and manages trusted users, detects network anomalies, identifies threats, and undertakes mitigation and response action. This group of technologies provide the ability for

cyberspace infrastructure to absorb the shock of a cyber-attack, identify adversary actions, respond with pre-determined actions, and ensure mission continuity.

(1) The Army, through use of these technologies as part of the DODIN-A and its supporting cyberspace infrastructure will assess, compose, and deploy cyberspace elements with known and predictable confidence in their identity, functionality, and content. These technologies further the development and deployment of autonomous smart-perimeter defenses consisting of access, transport, and integrity mechanisms that closely manage authentication of data, applications, and access. These technologies provide automated event detection in cyberspace and the IE to discover disinformation, propaganda, social hysteria propagation, crowd manipulation, and other events (such as a developing plan for cyberattack).

(2) Additional capabilities include those designed for alerting and warning of rapidly developing cyberspace and IE threats, actions, and events across multiple platforms. These technologies enhance a DODIN-A architecture designed to support data integrity in a holistically integrated way that reduces the capacity for threats to maneuver indiscriminately within cyberspace infrastructure and the IE.

g. Electromagnetic protection and electromagnetic camouflage. Electromagnetic protection and electromagnetic camouflage is the ability to protect vehicles against enemy multispectral sensors that can detect a variety of electromagnetic signatures. This multi-spectral camouflage would shield Army vehicles from near-infrared, shortwave infrared, medium-wave infrared, and long-wave heat-seeking sensors, as well as from RF and microwave radar waves and conceal objects from detection across several parts of the electromagnetic spectrum at the same time.

C-3. Advanced research and technology

a. Autonomous cognitive radio frequency (RF). A capability that provides a fully adaptive and reconfigurable RF architecture that is agnostic to waveforms. Though autonomous cognitive radio frequency is cognitive in nature, the Army will be heavily reliant on establishing standards to support the adaptive and reconfigurable RF architecture radios. These radios will operate autonomously and have the cognitive capability to operate in any frequency band supported by the hardware with any modulation using multiple access specifications, depending on the restrictions of the environment and overall EME operating conditions.

b. Quantum data processing. These technologies exploit quantum physics and associated phenomena at the atomic and sub-atomic scale. These technologies develop and deploy systems that can significantly outperform current computers and applications. Quantum data processing provide enhanced processing and computational capabilities enabling highly sophisticated approaches to encryption and decryption, along with sophisticated and rapid modelling and simulation that will enable complex operational and organizational decision making. The focus of these technological advancements is in cryptography, computation, precision navigation and timing, sensing and imaging, and communications. An effort focusing on Quantum electromagnetic sensing (e.g. Rydberg sensing) will greatly improve future Army sensing capacity.

c. Communications under extreme RF conditions. Provides technologies and techniques that address communications in degraded or contested EMS conditions. These technologies enhance the ability to cope with severe jamming and provide the capability to adapt to various jamming and interference sources. The technical objective is to innovate and integrate capabilities through all domains for adaptive interference suppression.

C-4. Breakthrough scientific discoveries and innovations statements

a. This section recommends a sub-set of breakthrough scientific discoveries and breakthrough technological innovations that support future cyberspace and EW operations in an integrated and synchronized manner to create and exploit windows of superiority within or across multiple domains, the EMS, and the IE to seize, retain, and exploit the initiative to defeat the enemy. The research efforts outlined in this section are a result of collaboration between the concept expertise about future operational needs and the technical expertise concerning use-inspired programs. Each breakthrough scientific discovery or breakthrough technological innovation effort is also linked to the required capability categories outlined in appendix B. This section will be revisited at least annually to reflect the anticipated and evolving needs associated with the Army cyberspace and EW force of 2028 to 2040.

b. Breakthrough technological innovations (RCs throughout are from this document).

(1) Research in sensitive RF detection sensors and automated detection algorithms will allow for the discovery of enemy passive RF detection systems, which lack an active signature. This capability will enable enemy systems detection and targeting when the system is not active so that it can be neutralized, destroyed, or manipulated. (RCs b, c, e, g, k, m, n, p)

(2) Research into reconfigurable and wideband antennas, transceivers, digital signal processors, and intelligent algorithms applied to the EME and cyberspace domains that autonomously create a complex and chaotic battlefield environment will allow commanders to manage the adversary's common operating picture. This advancement will enable commanders to seize, retain, and exploit the initiative by delaying the adversary's decision-making process and response time through increased chaos and uncertainty of friendly forces position and activity on the battlefield. (RCs a, c, d, e, h, k, n, o)

(3) Research into non-volatile random-access memory will enable atomic-scale processing applied to computer memory that can be written quickly and remain stable without a power supply for over 10 years. This capability will support distributed sensors and communications where information is processed at the tactical edge to increase situational awareness. (RCs a, b, c, g)

(4) Research into hardware and protocols for alternative communication modalities for both low probability of detection and classification will allow for secure, and resilient communications at all echelons. This advancement will enable integration of capabilities across all echelons and domains to achieve operational and strategic objectives. (RCs b, c, e, g, r, s, u)

(5) Research into enabling the continuation of data streams in DIL environments will enable the identification of technologies that adapt the data stream to the remaining bandwidth provided

by the network as it auto adjusts and adapts to existing conditions (such as weather, noise, jamming, and others) and reduce overall system latency of data delivery (under 0.1 secs). This advancement will enable networks with improved security and robustness, where data delivered to the end user is tolerant of periods of no data of more than a second, bandwidths below 10 kbps, and incomplete data feeds caused by noise (jamming, weather, and others), without disconnecting. (RCs a, b, c, e, h, l, m, r s)

(6) Research that links two approaches that use various taxonomies and variables to express imperfect information to model and represent uncertainty for different modalities of data (for example, sensor time series data, warfighter function tasks decision variables) and weighs the imperfect nature of the source information and influencing factors will begin to capture how commanders weigh information prior to a decision. The ability to capture uncertainty of information in possible courses of actions developed through artificial reasoning-based approaches such as this, will enable commanders to understand the negative outcomes associated with different courses of action. (RCs a, b, c, e, l)

(7) Research in advance integration of RF, cyberspace, acoustic, and electro-optical\infrared (EO/IR) to enable signature generation from a variety of sources distributed in the area of operations. The ability to generate multi-spectral, decoy signatures will enable friendly forces to deceive enemy sensors and obscure friendly forces and systems. (RCs d, e, h, k, l, o.)

(8) Research in the non-linear dynamics of RF circuit types in response to unconventional waveforms will provide the capability to introduce signals into hostile systems that can essentially take control of the system, with or perhaps without warning the operator, to spoof it, introduce false information, turn off, etc. Non-traditional EA will deceive enemy sensors by providing faulty data and denying the enemy's ability to sense and target friendly forces. (RCs a, e, g, k, l, n, o).

(9) Research in atom interferometry, including creation of macroscopic quantum superposition states, ways to prolong coherence, spin squeezing, entanglement creation, and ways to improve size, weight, and power and resilience of existing quantum sensors, will lead to more sensitive and robust sensors for electric, magnetic, electromagnetic and gravitational fields among other things. This advancement will enable both friendly and enemy signatures to be detected and monitored at unprecedented sensitivity in compact, resilient, and deployable packages, enabling by mid-term improved situational awareness, and in the long-term sensing orders-of-magnitude beyond what is possible from traditional sensors. (RCs c, e, g, i, l, m, o, p)

(10) Research into reciprocal and deterministic RF hardware and low-latency techniques/algorithms for time and phase synchronization of distributed transceivers will enable complex communication and resilient EW application of ground and air platforms to degrade adversary sensors and communications allowing for extended operations within anti-access and aerial denial environments. This advancement will enable non-lethal offensive EW options for commanders to shape the adversary's information environment, potentially leading to windows of opportunity. (RCs a, e, k, n, o)

(11) Research into threat-agnostic ES algorithms that identify transmitters and receivers based on intrinsic hardware characteristics and cognitive EA algorithms and concepts of

employment will enable threats to be addressed with no prior information or intelligence. This advancement will enable EAs that will learn through feedback from damage indicators and converge in real-time to more optimal attacks for new threats on the battlefield. (RCs e, k, m, n, p)

(12) Development of high-fidelity modeling, simulation, and emulation technologies to enable research and demonstration of real-time cognitive EW concepts and techniques in complex, highly realistic electromagnetic environments. This advancement will reduce the time of EW research and development, leading to resilient, threat-agnostic EW capabilities. (RCs c, h)

(13) Research into creation, maintenance, and distribution of entanglement will be the basis of future quantum networks containing, among other things, sensor nodes that will enable distributed quantum sensing for more advanced signature detection as well as time distribution. This advancement will enable sensing for more advanced signatures, including gradients and higher derivatives, to provide a more complete picture of the underlying structure of the field patterns being sensed, enabling enemy signatures to be detected and monitored around high-assets with unprecedented sensitivity; and clock synchronization for situational awareness, greater bandwidth communications and networking. (RCs c, g, p)

(14) Army forces will require capabilities to securely communicate in degraded or contested EMS conditions and while simultaneously conducting DCO and OCO.

(15) Research into extremely heterogeneous networking, which utilizes multiple diverse communication technologies and intelligent networking protocols, will increase the accessibility, availability, and resistance of the physical layer of the cyberspace domain. This advancement enables the establishment of a resilient and secure cyberspace infrastructure to enable successful MDO. (RCs b, e, g, r, s, u)

(16) Research into context-aware networking, which enhances network performance through exploitation and inference of multiple environmental contexts (network, mission, radio, threat) will support predictive, anticipatory adaptation of networked information, including intrusion alarms or anomalous behavior. This development will maximize the overall information capacity of networks that will adapt to changing mission requirements and limitations of the network environment, specifically enabling greater understanding of cyberspace threats in the network. (RCs b, c, e, g)

(17) Research into quantum computing will potentially lead to systems that can efficiently defeat currently deployed cryptographic protocols exponentially faster than the best-known classical methods. This advancement could lead to a decisive information advantage over the adversary and require significant defensive measures to protect against a potential quantum-enhanced adversary. (RCs a, b, c, g, l, r, s)

(18) Research into distributed quantum protocols for collaboration and decision making include quantum secret sharing; in this process information is effectively ‘distributed’ among several users such that the determination of the ‘secret’ requires the collaboration of a subset of users and attempts to eavesdrop are detectable through the unavoidable introduction of errors. This

capability will enable the secure communication of sensitive and critical information between verified participants. (RCs r, s, t, u)

(19) Research into distributed quantum computing will enable coherent networking (i.e., quantum networking) of multiple quantum computers that are not geographically co-located and together perform calculations infeasible on any single system in the network. Advances in distributed quantum computing, and quantum computing, in general, may enable processing and computational capabilities that can perform specific calculations more efficiently than the best-known classical alternatives for applications such as decryption of specific standard encryption protocols. (RCs a, b, c, g, l)

(20) Research into blind quantum computing will enable encoded computations, where the mainframe will not be aware of the specific calculation being performed and thus cannot eavesdrop on the results of the calculation; additionally, some versions of blind quantum computing also ensure the integrity of the computation and hence rule out malicious tampering. Blind quantum computing would prevent attempts for deception through these means by the adversary and would enable computing to run securely even on an untrusted quantum mainframe (that is, owned by a public company or located in another country). (RCs r, s, t, u)

(21) Research into quantum key distribution will enable quantum channels to be used to generate shared secret keys between two users, where any eavesdropping or meddling can be detected, and the security of the keys is certified in the process that produces them. These keys, which can then be stored on classical hardware and used as one-time pads for secure classical communication that are not susceptible to a quantum attack, will enable secure transmission of information in support of MDO. (RCs r, s, t, u)

(22) Research into network agility enhances autonomous DCO and resilience through theories and techniques to direct proactive cyberspace maneuvers that consider various network characteristics, topologies, and platforms to support and improve machine-learning techniques that evaluate multiple cost (that is, performance) and security tradeoffs within Army networks. This research will not only offer commanders more options to achieve operational goals but will also contribute to better autonomous planning and control of cyber maneuvers, and increased capability to deceive adversaries and protect Army cyberspace assets. (RCs b, c, e, h, i, l, r, s, u)

(23) Research in detection of cyberspace threats, which enhances situational understanding of the network through decentralized, distributed monitoring and vulnerability/attack analysis, will support autonomous, adaptive protection of Army cyberspace infrastructure. This development will improve the robustness and resilience of the network in the face of dynamic mission requirements and powerful adversaries. (RCs b, c, e, i, r, s, t)

(24) Research in dynamic honeynets improves robustness of cybersecurity through development of strategic approaches and technical capabilities to generate synthetic aspects of the cyberspace domain, including generation of network topologies, users, information, services, and profiles. This research will provide additional DCO capabilities enabling better understanding of adversarial intent and capabilities as well as enhanced strategies to mitigate the impact of adversarial attacks. (RCs b, c, d, g, h, i, n, r)

(25) Research into adversarial machine learning (AML) enhances cybersecurity resilience through development of attacks and defenses against advanced machine learning employed in the cyberspace domain, such as intrusion detection, network traffic classification, and firewalls. This research will enable military operations to leverage AML and machine learning advances for the cyberspace domain to understand vulnerabilities of ML systems and harden hosts against emerging and evolving AML threats. (RCs a, b, c, e, g, i, n, r)

(26) Army forces will require the integration of AI and machine learning to support OCO and EA to increase decision-making speed beyond human capability.

(27) Research to transform raw and processed data into actionable information, where causal inference is used to aid in determining components, objects, and signals from different modalities with complex relationships to aid in forming the "best" hypothesis, will enable the generation of courses of action and present uncertainty of information. Advances in reason-based decision making will enable commanders to quickly recognize and act upon opportunities to seize the initiative. (RCs a, b, c, e, l)

(28) Research in opportunistically sensing Soldier intent and interest coupled with advancing methodologies to sense and interpret Soldier behavior in the real-world environments are enabling AI to use the human brain to prioritize tactically critical information without providing any additional burden or stress on the operator. Tactical situational understanding via collective knowledge will allow blue force AI to infer and integrate the intent of Soldiers as it evolves with mission execution and create a form of super-human intelligence that leverages the tactical knowledge of Soldiers with the speed and processing power of AI. (RCs a, b, e, l)

(29) Research on multi-timescale models of individual humans and machine learning based predictions of future human behaviors will enable AI to infer human information processing performance and will allow for future AI to weight inputs from multiple humans in making decisions. AI-inferred human long-timescale processing will allow blue force future AI to have mechanisms to non-linearly improve its integration of Soldier intelligence into mission planning and asset coordination. (RCs a, b, e, l)

(30) Research on context-aware information filtering integrated with advanced visualization technology, where high-performance computing infrastructure is leveraged to analyze the data streams at multiple levels of context, prioritize, and visualize the analyzed data in a variety of mediums, will enable rapid decisions through the production of actionable information. This advancement will enable the integration and consumption of large quantities data, spanning multiple data types, while reducing cognitive overload. (RCs a, b, c, e, l)

(31) New advancements in distributional semantics, ontological representations, data mining and representational learning are enabling the training of information extraction with limited annotations and the automatic extension of ontologies. This advancement will enable the development of robust and accurate information extraction and querying systems that can process unstructured textural data from new and rapidly evolving areas of knowledge with limited data,

which will lead to improved commanders' situational understanding in all operational environments. (RCs a, b, c, e, l)

(32) Research to exploit knowledge of human spatial reasoning neural systems which have hundreds of different sub-architectures to AI, which currently has one of those sub-architectures, to develop a completely novel class of AI will revolutionize AI spatial reasoning capabilities. Advancements in neuro-derived AI will lead to a variety of new operational capabilities in areas such as data analytics that will have human-like reasoning, but function at a rate faster than humanly possible. (RCs a, b, e, l)

(33) Research in algorithms and communication approaches for developing, maintaining, and sharing situational awareness across and between humans and AI distributed across echelons are leading to the creation of mechanisms to understand gaps and inconsistencies in information flow and communications underlying decision making. Shared Human-AI awareness will allow future forces to enhance shared situational awareness throughout the competition continuum. (RC c)

(34) Research into the use of deep reinforced learning will enable four different capabilities in multi-domain operations: create and exploit potential windows of superiority during deliberate planning; continually sense, identify, and quickly exploit emerging windows of superiority; continually sense and identify emerging windows of vulnerability; and respond to individual user differences and drive customized knowledge management. These advancements will support decision making at all echelons in planning, preparing, executing, and assessing operations across the competition continuum and enable the US Army to achieve disruptive Warfighting capabilities. (RCs a, b, c, e, l)

Appendix D
Dependencies

D-1. Introduction
This appendix identifies the dependencies on other functions required to perform the capabilities identified in this concept.

D-2. Dependencies on other warfighting functions

a. Cyberspace and EW operations are conducted to support joint and Army operations. This support provides methods for other operations such as IO, intelligence, and space to enable or utilize cyberspace and EW operations to execute their core missions. Commanders and staffs consider how other operations affect or utilize cyberspace and the EMS while simultaneously maintaining awareness of how actions undertaken in cyberspace and the EMS may impact other operations, functions, missions, and tasks. The broad impact of cyberspace and EW operations must be considered when planning and conducting all operations.

b. Operations within the other four domains as conducted by warfighting and supporting functions are dependent on cyberspace and EW. Conversely, cyberspace and EW are dependent upon the other four domains and the warfighting and supporting functions to conduct operations. Operations in cyberspace rely on the links and nodes that exist in the natural domains. Operations

in the other domains create effects in and through cyberspace by affecting the EMS, the data, or the physical infrastructure.

D-3. Intelligence

Cyberspace and EW operations are dependent upon intelligence to provide support through the application of the intelligence process, IPB, and information collection. Intelligence at all echelons supports DODIN operations, DCO, and OCO planning and assists with defining measures of performance and measures of effectiveness. The intelligence process leverages all sources of information and expertise, including the intelligence community and non-intelligence entities to provide situational understanding. Information gathered provides insight into enemy activities, capabilities, motivations, and objectives and enables the planning, preparation for, and execution of cyberspace and EW operations. Cyberspace and EW planners need to leverage intelligence reach, analysis, reporting, and production capabilities provided by the intelligence warfighting function to provide cyberspace and EW effects.

D-4. Space

a. The relationship between the space and cyberspace domains is unique. Space operations depend on the EMS for the transport of information and the control of space assets. Space operations provide specific capability of transport through the space domain for long haul and limited access communications. Space provides a key global connectivity capability for cyberspace and EW operations. Additionally, cyberspace and EW operations provide a capability to execute space operations. This interrelationship is an important consideration across cyberspace operations, and particularly when conducting targeting in cyberspace.

b. Many cyberspace and EW operations occur in and through the space domain via the EMS, resulting in an interdependent relationship between space and cyberspace. Space operations and the capabilities, limitations, and vulnerabilities of space-based systems affect support to cyberspace and EW operations.

c. Cyberspace operations are dependent on Space to provide global access through satellite communications. While satellite communications provide links as part of the DODIN, the nature of satellite operations makes them significantly different from other terrestrial or air-based communications systems. Similarly, space relies on cyberspace and the EMS for command and control of satellite systems and associated ground nodes. Cyberspace and EW operations rely on space-based capabilities that provide satellite communications, ISR, positioning navigation and timing, and space control.

D-5. C2

Cyberspace and EW forces and operations are dependent upon C2 to integrate cyberspace and EW operations with the other warfighting and support functions and to create necessary shared understanding. This dependency is critical to cyberspace and EW forces to plan, communicate, navigate, maneuver, and maintain battlefield situational understanding. C2 is essential to effectively synchronizing IRCs and conducting cyberspace electromagnetic activities.

D-6. Maneuver
Cyberspace and EW forces and operations are dependent upon maneuver to place cyberspace and EW forces in position to support MDO. Cyberspace and EW forces utilize elements of the movement and maneuver warfighting function to position forces for offensive and defensive operations and reacting to meeting engagements.

D-7. Fires
Cyberspace and EW forces and operations are dependent upon fires for support through the targeting process and the suppression or destruction, under certain operational scenarios, of adversary cyberspace and EW assets. Crucial to the successful employment of cyberspace and EW capabilities is fires ability to provide a fire support coordination capability that integrates all fires, including cyber and EW. Key to maximizing cross-domain synergy will be fielding a system for planning, requesting and directing all available fires so any element of a Joint Force can access the most appropriate supporting arm.

D-8. Protection
Cyberspace and EW forces and operations are dependent upon protection for physical and general force protection measures. Protection of cyberspace and EW assets is complicated by their logical connectivity that can enable enemies to create multiple, cascading effects that may not be restricted by physical geography and civil/military boundaries. Key to cyberspace protection is the positive control of all direct connections between the DODIN and the Internet and other public portions of cyberspace, as well as the ability to monitor, detect, and prevent the entrance of malicious network traffic and unauthorized exfiltration of information through these connections.

D-9. Sustainment
Cyberspace and EW forces and operations are dependent upon sustainment for all supply requirements. Army forces need the capability to adapt by rapidly incorporating new cyberspace capabilities into their arsenal. This will require a highly technical supply chain with an emphasis on high-speed software distribution and enhanced technical innovation mechanisms that integrate advanced technology into existing cyberspace infrastructure quickly and seamlessly. Additionally, the Army forces may need the capability to quickly upgrade their own cyberspace and EW capabilities to leverage these new technologies.

D-10. SOF
Cyberspace and EW forces and operations are dependent upon special operations capabilities, under certain operational scenarios, to gain access to adversary systems in challenging and fluid operational environments. In competition and conflict, special operations forces provide the necessary access and placement required to strike adversary critical capabilities in areas where either physical or domain access is denied.

D-11. Aviation
Cyberspace and EW forces and operations are dependent upon aviation for extended range capability through the use of aviation platforms. This capability is especially significant with regard to EW where distributed access range extension through aerial layer network capabilities is significant to long range sensing.

Appendix E
Contributions to Competition

a. Competition is critical to the successful execution of cyberspace and EW operations as well as to the overall success of MDO. The Army uses cyberspace and EW operations in support of OIE to shape the OE. Army forces seize the initiative in competition by using cyberspace and EW operations to converge IRCs with operations, throughout all echelons and across all domains. This allows the Army to execute tailored actions aggressively to employ cyberspace and EW operations along with IW and engagement operations to counter and expose inconsistencies in the adversary's information narratives. During competition, the Army must deter conflict, prevent the adversary from expanding competitive space in all domains, and enable the rapid transition to conflict. The Army will prioritize securing sensitive information and deterring adversary malicious cyberspace and IW activities designed to threaten the U.S., allies, and partners. Cyberspace and EW operations during this phase are active to set the theater.

b. Cyberspace and EW operations during competition aid in establishing a robust operational assessment of the adversary's forces and capabilities that ensures the Army can rapidly transition to conflict in response to aggression. The Army competes successfully by defeating the adversary's attempts to destabilize regional security and deterring armed conflict through a series of mutually reinforcing actions in and through all domains and the IE through the creation of singular and combined effects achieved through integration and synchronization of warfighting capabilities and IRCs. Along with mission partners, ARSOF, proxies, and surrogates Army forces using cyberspace and EW operations to support IW and engagement operations, counter the adversary's information narratives and conduct deception to create uncertainty within an adversary's decision-making process. Consideration should be afforded towards integrating operations with the Special Operations Joint Task Force (SOJTF) and ARSOF tactical elements operating in the deep fires area. ARSOF provides options for Army and the joint force which can advance enduring partner relationship, influence adversarial behavior, generate strategic options to understand the problem, and conduct integrated decisive operations across the space of competition and conflict.

c. The Army counters adversary cyberspace and EW campaigns threatening U.S. military advantage by defending forward to intercept and halt cyberspace and EW threats and by strengthening the security of cyberspace infrastructure that supports MDO missions. Due to the increasing importance of cyberspace, EW, and information the Army moves beyond the current operations model focused primarily on physical power and uses cyberspace and EW operations as tools of informational power to shape environments and engage adversary systems and networks as part of an aggressive strategy to shape, deter, and defend.

d. The Army uses cyberspace and EW operations in support of OIE to conduct deception by manipulating information across the human, physical, and informational dimensions that complicates the adversary's ability to determine friendly force capability and capacity. While physical signs of exercises, training, and alerts demonstrate specific capabilities, they also provide opportunities to mislead the adversary regarding the disposition and staging of forces using various methods (such as, multi-media, the EMS, cyberspace, data encryption, network access limitations,

and decoy data). These actions create unpredictability and complicate the adversary's reconnaissance efforts, which increases the likelihood of compromising its assets.

e. During the competition period, commanders base their planning and decisions on a continually evolving understanding of the OE. Integrated cyberspace, EW, and SIGINT capabilities collect against and analyze adversary operational and tactical systems, as well as other facets of the OE and civil networks. When fused with broader information and intelligence collection operations, these efforts build the necessary data sets that allow a commander to visualize the three-dimensional, multi-domain environment at a detailed level for operational planning and mission execution. Collectively, these actions enable Army forces to rapidly transition to conflict and create uncertainty for the adversary as to whether it can achieve its objectives through conflict.

f. Through shaping the OE and addressing aggression, cyberspace and EW operations provide a credible deterrent, while commanders calibrate force posture to reduce an adversary's local military superiority, employ multi-domain formations to withstand an attack, and demonstrate the ability to converge forward presence, joint, and national-level capabilities to disrupt any attack. The exercise of directions (C2) facilitated by decentralized execution (mission command) is time and situationally sensitive. During the transition period from competition, and during conflict, the OIE strategy must fully utilize the cross domain and near real time advantage cyberspace and its associated concepts can provide.

Appendix F
Contributions to Conflict

a. The Army deters adversaries by operating and maintaining strong cyberspace and EW operations capabilities. If deterrence fails, Army forces isolate, overwhelm, and defeat adversaries in cyberspace, the EMS, and the IE to meet the commander's objectives. Commanders employ cyberspace and EW operations capabilities to deceive, degrade, disrupt, deny, destroy, or manipulate across multiple domains. Cyberspace and EW operations also create cascading effects across multiple domains to affect weapons systems, command and control processes, critical infrastructure, and key resources to outmaneuver adversaries physically and cognitively.

b. Cyberspace and EW operations facilitate maneuver in and through all domains, the EMS and the IE across strategic, operational, and tactical distances enhancing combat power while setting the conditions for the defeat of the enemy's conventional, unconventional, and IW capabilities resulting in a decisive advantage and freedom of maneuver. Cyberspace and EW operations support the immediate contest of the IE by supporting an OIE strategy that contains a credible and compelling message to bolster friends, placate neutral populations, and deny adversary IW objectives. These plans include prepared messages and methods of delivery based on anticipated wartime conditions, such as disruptions to civilian media and energy networks.

c. Commanders employ cyberspace and EW capabilities to deceive, degrade, disrupt, deny, destroy, or manipulate across multiple domains (see note 1). These capabilities exploit adversary systems to facilitate intelligence collection, target adversary cyberspace and EMS capabilities, and create multi-domain effects. Army forces capitalize on operations conducted during competition

to engage adversary strategic and operational stand-off by immediately neutralizing the adversary's long-range systems, contesting adversary maneuver forces in all domains, the EMS, and the IE. Cyberspace and EW operations converge capabilities to optimize the generation of effects across multiple domains against critical components of adversary A2AD systems. Cyberspace and EW operations provide steady delivery of layered capabilities through multiple domains, the EME, and the IE to enable commanders to stimulate, see, and strike adversary A2AD systems.

d. Army cyberspace and EW forward presence and expeditionary forces enable the rapid defeat of aggression through a combination of integrated capabilities, scalable formations, and cyberspace infrastructure to immediately contest an adversary attack in depth. Forward positioned EW forces immediately contest the adversary attack by conducting EA against adversary maneuver forces and through disruption of adversary actions in cyberspace, the EMS, and the IE. Friendly EA and OCO focus on degrading or denying adversary command, control, communications, computer, intelligence, surveillance and reconnaissance systems and infrastructure to open windows of advantage for maneuver.

e. Cyberspace and EW operations overmatch adversary capabilities at critical times and places to achieve windows of superiority. Cyberspace and EW operations support SIGINT and geospatial intelligence (GEOINT) assets focused on target refinement to support the targeting process and provide targets for cross domain effects. The adversary's intelligence and information collection-to-fires networks are a critical capability to identify and locate as targets. Cyberspace and EW operations effectively exploit their integrated capabilities to inhibit the adversary's use of the EMS and their C2 networks.

f. The Army conducts cyberspace and EW operations to support the opening of additional lines of operations or to establish initial entry points to enable follow-on actions. Aggressive employment of cyberspace and EW operations create multiple means to limit adversary situational understanding and present the adversary multiple real and perceived dilemmas that produce uncertainty within their decision cycle resulting in decreased operational effectiveness. Cyberspace and EW forces support friendly force deception measures and IW operations while EW forces provide deceptive emissions to mask friendly force EMS capabilities, as well as suppress adversary capabilities such as communications and radars.

g. The Army adapts to changing conditions in the OE and IE through an understanding of the linkage between ongoing maneuver operations, cyberspace, EW, and the application of other information-related effects, while assessing their impact on OIE. The Army must understand, block, and counter adversary use of ideas, images, and violence designed to manipulate the U.S. and mission partners. Army forces integrate and synchronize emerging technical capabilities with socio-cultural analysis to support IW and information engagement operations, in a sustained approach, to enable freedom of maneuver within and across all domains and the IE.

Appendix G
Contributions to Returning to Competition

a. Army forces use cyberspace capabilities to maintain psychological, technological, temporal and spatial advantages over the adversary. The Army counters cyberspace and EW threats, mitigates degraded access to cyberspace and the EMS, and takes actions against enemy cyberspace and IW capabilities to achieve and maintain positions of advantage. Cyberspace, EW, and SIGINT monitoring are synchronized to maximize effective and efficient use of assets. Cyberspace and EW operations provide prioritization and coordination of available spectrum and bandwidth within the EMS in support of OIE.

b. Cyberspace and EW operations contribute to the consolidation of strategic gains after conflict through the application of non-lethal and information-related effects that support securing the initiative and the maintenance of operational contact in all domains, the EME, and the IE. Cyberspace and EW operations block adversary IW tactics by reinforcing compelling narratives through support of deliberate, focused, and sustained information engagement operations designed to promote cooperation and to reassure allies and partners.

c. EW operations assist local governments with spectrum management operations as appropriate. Cyberspace operations also re-establish critical cyberspace infrastructure and connections to critical nodes to facilitate delivery of messaging in support of OIE. Cyberspace and EW forces maintain positions throughout the OE to provide continuous situational understanding, and conduct EA, EP and OCO to counter adversary messaging as required. DCO continues to provide protection for critical nodes and cyberspace infrastructure. During re-competition cyberspace and EW forces, along with intelligence and space assets, locate targets, support force protection, and provide indications and warnings.

d. Cyberspace and EW forces in conjunction with other warfighting and support functions provide layered space, SIGINT and ES coverage to detect EMS use by adversary elements in accordance with negotiated host-nation agreements. Army forces conduct EA and OCO to deny the adversary use of friendly and host nation EMS. Integrated SIGINT, EW, and cyberspace operations support partner governments to re-establish essential services and governance.

e. Army forces conduct cyberspace and EW operations to retain the advantage and secure key terrain and friendly populations. Aggressive cyberspace and EW operations in support of OIE consolidate gains by influencing friendly and adversary civilians, militaries, and governments. At the same time, cyberspace and EW operations support ARSOF in the conduct of unconventional warfare with unified action partners, proxies, and surrogates while providing continued support to friendly forces in deterring adversary conventional attacks. The consolidation of gains, reconstitution of friendly cyberspace and EW forces, and building the cyberspace and EW capacity of partners enables long-term deterrence. Special consideration should be afforded towards integrating operations with the SOJTF and ARSOF tactical elements employed in consolidating gains through the hardening of partner infrastructure and friendly networks.

f. Army cyberspace and EW operations set conditions for long-term deterrence by regenerating and expanding both Army and partner capacity. Cyberspace and EW operations use defensive planning and preparation to deter a return to conflict providing space and time to build enhanced capability and interoperability with partner forces. Through a successful transition from conflict

to the return to competition, integrated cyberspace and EW operations translate operational success in conflict to the attainment of strategic objectives.

g. Figures G-1 and G-2 are representative of cyberspace and EW support to MDO but should be considered as illustrative only. Actual force structure and capabilities are classified.

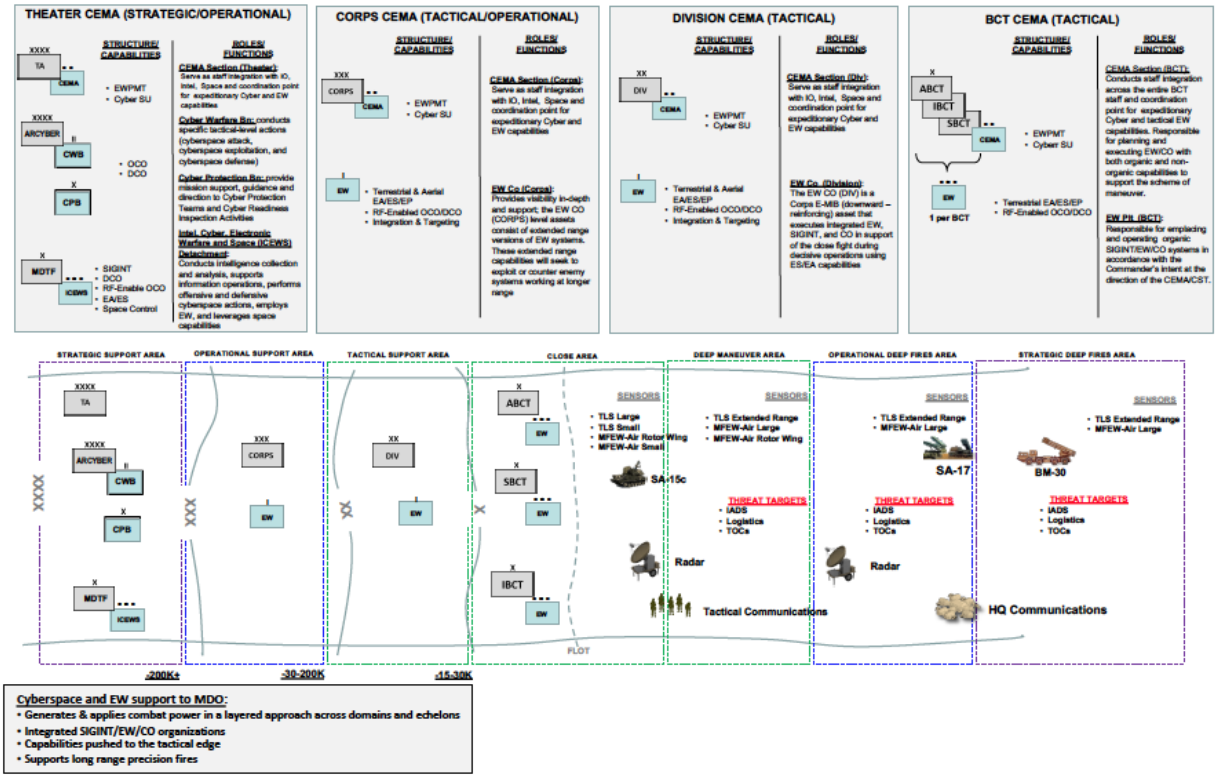


Figure G-1. Cyberspace and EW support to MDO

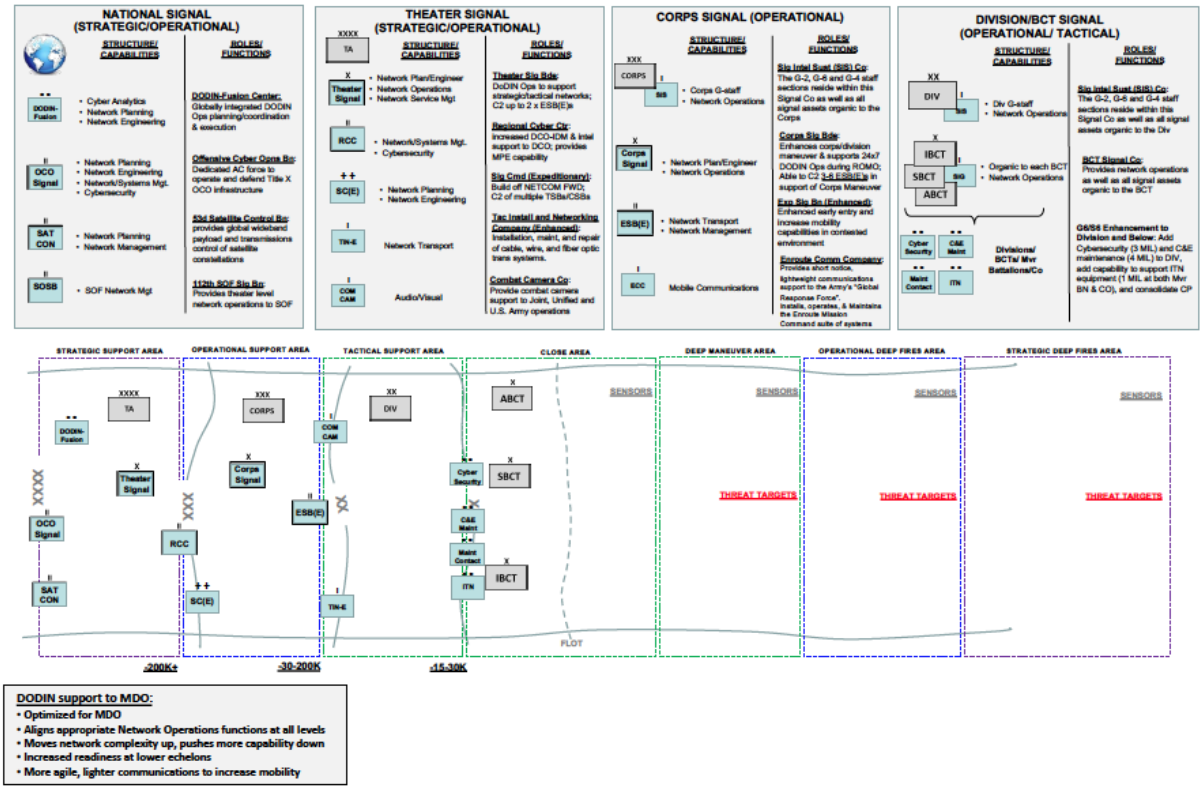


Figure G-2. DODIN support to MDO

Appendix H
Authorities

a. Army forces conduct cyberspace and EW operations as part of the Joint force. Army forces may conduct OCO, DCO, and EW with Army organic or joint requested effects to support the joint commander's intent. United States Cyber Command has overall responsibility for directing DODIN operations and defense. U.S. Army Cyber Command (ARCYBER) conducts DODIN-A operations and DCO within Army networks, and when directed, within other DOD and non-DOD networks.

b. Army forces conduct operations directed by the President while adhering to appropriations, authorizations, and statutes as provided by Congress. These statutes cover wide areas of the law including domestic security, the regulation of the Armed Forces, Federal crimes, the National Guard, information technology acquisition and service, electromagnetic spectrum management, and intelligence.

c. The following statutes are applicable to cyberspace and EW operations. This list is not to be considered complete and all statutes and authorities are subject to change, Presidential direction, and Congressional oversight.

(1) Domestic Security, USC Title 6. Establishes responsibilities for information analysis and infrastructure protection, chief information officers, and cybersecurity oversight. USC Title 6

responsibilities include comprehensive assessments of key resources, critical infrastructure vulnerabilities, and identifying priorities for protective and supportive measures regarding threats. (For more information, see U.S. Code Title 6.)

(2) The Armed Forces, USC Title 10, Enables the Army to organize, train, equip, and provide land, cyberspace operations, and EW units and headquarters. USC Title 10 authorities and restrictions provide context and foundation for how the Secretary of Defense directs military cyberspace operations, EW, and military intelligence operations.

(3) Crimes and Criminal Procedure, USC Title 18. Army forces conduct cyberspace operations and EW in compliance with Federal law and takes measures to ensure operations respect the rights of persons against unlawful searches and seizures pursuant to the 4th Amendment. Coordination with the Army Criminal Investigation Division ensures appropriate investigation of criminal activity on the DODIN under Title 18 authorities. USC Title 18 includes those crimes conducted in cyberspace.

(4) The National Guard, USC Title 32. National Guard units are state military units which are equipped and trained pursuant to Federal statutory authorization. The National Guard may conduct missions for their state but paid for by the Federal government under USC Title 32, if the Secretary of Defense determines the mission is in the interests of the DOD.

(5) Information Technology Acquisition, USC Title 40, Ch. 113, is applicable to the Army and all Federal agencies. USC Title 40 establishes the responsibilities of the agency heads and agency chief information officers and guidance for acquisition of information technology.

(6) USC Title 44, Public Printing and Documents establishes responsibilities of agency heads for statutory requirements and authority for ensuring information security and information resource management. This includes information security in cyberspace.

(7) Telecommunications, USC Title 47, prescribes the statutory requirements and authority for access to, and use of, the EMS within the United States and Possessions to Federal agencies. The chief information officer/assistant chief of staff, signal (G-6), as outlined in AR 5-12, implements national, international, DOD, joint, host nation, and Headquarters, Department of the Army spectrum management policies and guidance throughout the Army. In this capacity, the chief information officer/G-6 ensures compliance with 47 USC as well as other applicable Federal, DOD, and military department EMS governance and policy to minimize radio frequency interference at DOD and Service test ranges and installations for activities such as GPS testing and EA clearances for training, testing, and evaluating.

(8) War and National Defense, USC Title 50, provides authorities concerning the conduct of both military and intelligence activities of the U.S. Government. Intelligence activities conducted by the U.S. Government must be properly authorized, conform to the U.S. Constitution, and be conducted under presidential authority. Executive Order 12333 establishes the framework and organization of the intelligence community as directed by the President of the United States. For example, the order directs the NSA as the lead for signals intelligence. DOD policy documents,

including DoD Manual 5240.01, "DoD Intelligence Activities," establish DOD policy for the conduct of intelligence operations.

(9) The Army strictly limits and controls collection of information on U.S. persons and collection in the United States. AR 381-10 identifies the types, means, and limitations concerning collection retention and dissemination of information in the United States and on U.S. persons. This regulation applies to cyberspace within the boundaries of the United States and U.S. persons abroad.

Glossary

Section I
Abbreviations

AFC	Army Futures Command
AI	artificial intelligence
AML	adversarial machine learning
APT	advanced persistent threats
ARCYBER	Army Cyber Command
ARSOF	Army special operations forces
C2	command and control
CE	computing environment
CFT	Cross Functional Team
COE	common operating environment
CONOPS	concept of operations
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations-internal defensive measures
DIL	degraded, intermittent, limited
DOD	Department of Defense
DODIN	Department of Defense information network
DODIN-A	Department of Defense information network-Army
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, policy
EA	electromagnetic attack
EM	electromagnetic
EME	electromagnetic environment
EMS	electromagnetic spectrum
EP	electromagnetic protect
ES	electromagnetic warfare support
EW	electromagnetic warfare
FCC	Futures and Concepts Center
IE	information environment
IPB	intelligence preparation of the battlefield
IRC	information-related capability
ISR	intelligence, surveillance, and reconnaissance

IW	information warfare
JP	joint publication
MDO	multi-domain operations
OCO	offensive cyberspace operations
OIE	operations in the information environment
OPE	operational preparation of the environment
PTE	persistent training environment
RC	required capability
RF	radio frequency
S&T	science and technology
SMO	spectrum management operations
SOJTF	Special Operations Joint Task Force
SU	situational understanding
TP	TRADOC Pamphlet
TRADOC	Training and Doctrine Command
U.S.	United States
USC	United Stated Code

Section II
Terms

Army Special Operations Forces.
Those Active and Reserve Component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. Also called ARSOF. (JP 3-05)

combat power
Total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time. (ADP 3-0)

commander's intent
A clear and concise expression of the purpose of the operation and the desired military end state that supports C2, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned. (JP 3-0)

command post
A unit headquarters where the commander and staff perform their activities. (FM 6-0)

common operational picture
Single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command. (ADP 6-0)

conflict

When the use of violence is the primary means by which an actor seeks to satisfy its interests. (TP 525-3-1)

cybersecurity
The prevention of damage to, protection of, and restoration of computers, Electromagnetic communications systems, Electromagnetic communications services, wire communication, and Electromagnetic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DOD instruction 8500.01)

cyberspace
Global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02).

cyberspace operations
The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 1-02)

cyberspace superiority
The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 3-12)

data
(Army) Unprocessed signals communicated between any nodes in an information system or sensing from the environment detected by a collector of any kind (human, mechanical, or Electromagnetic). (ADP 6-0)

data management
Comprises all disciplines related to managing data as a valuable, organizational resource; the process of creating, obtaining, transforming, sharing, protecting, documenting and preserving data. (FM 6-02)

defensive cyberspace operations
Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 3-12)

defensive cyberspace operations -response actions
The deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DOD cyberspace capabilities or other designated systems. (JP 3-12)

degraded cyberspace environment
Any condition that reduces the effectiveness, stability, or availability of cyberspace infrastructure essential to the conduct of operations. (Proposed)

degraded information environment
Any condition that adversely affects the availability, timeliness, accuracy, or integrity of information essential to the conduct of an operation. (Proposed)

Department of Defense information network
The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, and security services, other associated services, and national security systems. (JP 6-0)

Department of Defense information network-Army
Core cyberspace infrastructure that Army forces are responsible for that is required to establish information networks and support cyberspace operations. (FM 6-02)

Department of Defense information network operations
Operations to design, build, configure, secure, operate, maintain, and sustain DOD networks to create and preserve cybersecurity on the DOD information network. (JP 1-02)

electromagnetic spectrum management
Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. (JP 6-01)

electromagnetic operational environment
The background electromagnetic environment and the friendly, neutral, and adversarial electromagnetic order of battle within the electromagnetic area of influence associated with a given operational area. (JP 6-01)

electromagnetic attack
Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-85)

electromagnetic protect
Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability. (JP 3-85)

electromagnetic support
Actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. (JP 3-85)

electromagnetic warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-85)

host nation
A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory. (JP 3-57)

information advantage
The application of information capabilities, including space, cyberspace, EMS, and influence, resulting in comparative advantage to support all domain operations. It includes intense targeting of adversary command and control, intelligence, surveillance, reconnaissance, and targeting. In the decision cycle, information advantage provides the ability to acquire, process, and present contextually relevant information from across all domains for action faster than an opponent. (Current CJCS working description)

information environment
The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13\JP 3-85)

information management
An organizational program that manages the people, processes and technology that provide control over the structure, processing, delivery and usage of information required for management and business intelligence purposes. (FM 6-02)

information operations
The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries (JP 3-13).

information requirement
(Army) Any information element the commander and staff must possess to successfully conduct operations. (ADP 6-0)

information services
To collect, process, store, transmit, display, and disseminate information. These services also support joint, interorganizational, and multinational collaboration. Information sharing allows mutual use of information services or capabilities. Shared capabilities sometimes cross functional or organizational boundaries. (FM 6-02)

integration
The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 1)

intelligence preparation of the battlefield/battlespace
A systematic process of analyzing and visualizing the portions of the mission variables of threat/adversary, terrain, weather, and civil considerations in a specific area of interest and for a specific mission. (ATP 2-01.3, JP 2-01.3)

joint electromagnetic spectrum operations
Those activities consisting of electromagnetic warfare and joint electromagnetic spectrum management operations used to exploit, attack, protect, and manage the electromagnetic operational environment to achieve the commander's objectives. (JP 6-01)

multi-domain operations
Cross-domain operations that create windows of superiority across multiple domains, and allow Joint Forces to seize, retain, and exploit the initiative. (TRADOC Pamphlet 525-3-1)

offensive cyberspace operations
Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 1-02)

operational environment
A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

operational preparation of the environment
The conduct of activities in likely or potential areas of operations to prepare and shape the operational environment. (JP 3-05)

organic
Assigned to and forming an essential part of a military organization as listed in its table of organization for the Army, Air Force, and Marine Corps, and are assigned to the operating forces for the Navy. (JP 1)

planning
The art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. (ADP 5-0)

preparation
Activities performed by units and Soldiers to improve their ability to execute an operation. (ADP 5-0)

situational understanding
The product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables to facilitate decision making. (ADP 5-0)

Special Operations Joint Task Force
Special Operations Joint Task Force. A SOJTF is a deployable, JTF-capable, headquarters that supports joint all domain operations and Army MDO. The SOJTF can be tailored for a range of operations from crisis response or limited contingency during competition to a joint force special operations component command (JFSOCC) for armed conflict. (JP 3-05)

spectrum management operations
Consist of the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the EME, during all phases of military operations. (FM 3-12)

stand-off
The physical, cognitive, and informational separation that enables freedom of action in any, some, or all domains, the electromagnetic spectrum, and IE to achieve strategic and/or operational objectives before an adversary can adequately respond. It is achieved with both political and military capabilities. (TRADOC Pamphlet 525-3-1)

synchronization
The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. (TRADOC Pamphlet 525-3-1)

system
A group of interacting, interrelated, and interdependent components or subsystems that form a complex and unified whole. Systems have a purpose with their parts arranged in a way (structure) to carry out their purpose. (TRADOC Pamphlet 525-3-3)

Section III
Special terms

information advantage*
The application of information capabilities, including space, cyberspace, EMS, and influence, resulting in comparative advantage to support all domain operations. It includes intense targeting of adversary command and control, intelligence, surveillance, reconnaissance, and targeting. In the decision-making cycle, information advantage provides the ability to acquire, process, and present contextually relevant information from across all domains for action faster than an opponent.

information-related capabilities (IRC)
Tools, techniques, or activities employed within a dimension of the IE that can be used to create effects and operationally desirable conditions. (DOD Dictionary).

joint information function
The function that helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. Furthermore, the function solidifies a Joint Force perspective recognizing the need for informational power by making its generation, preservation, and application through OIE the commander's business—similar to the other six existing functions. (DOD)

operations in the information environment (OIE)
Actions taken to generate, preserve, and apply informational power toward a relevant actor in order to: inform or influence, increase or protect a competitive advantage or combat power potential, within the operating environment. OIEs span the competition continuum (cooperation, competition short of armed conflict, and warfighting). (TRADOC Pamphlet 525-3-3)

* Proposed definition