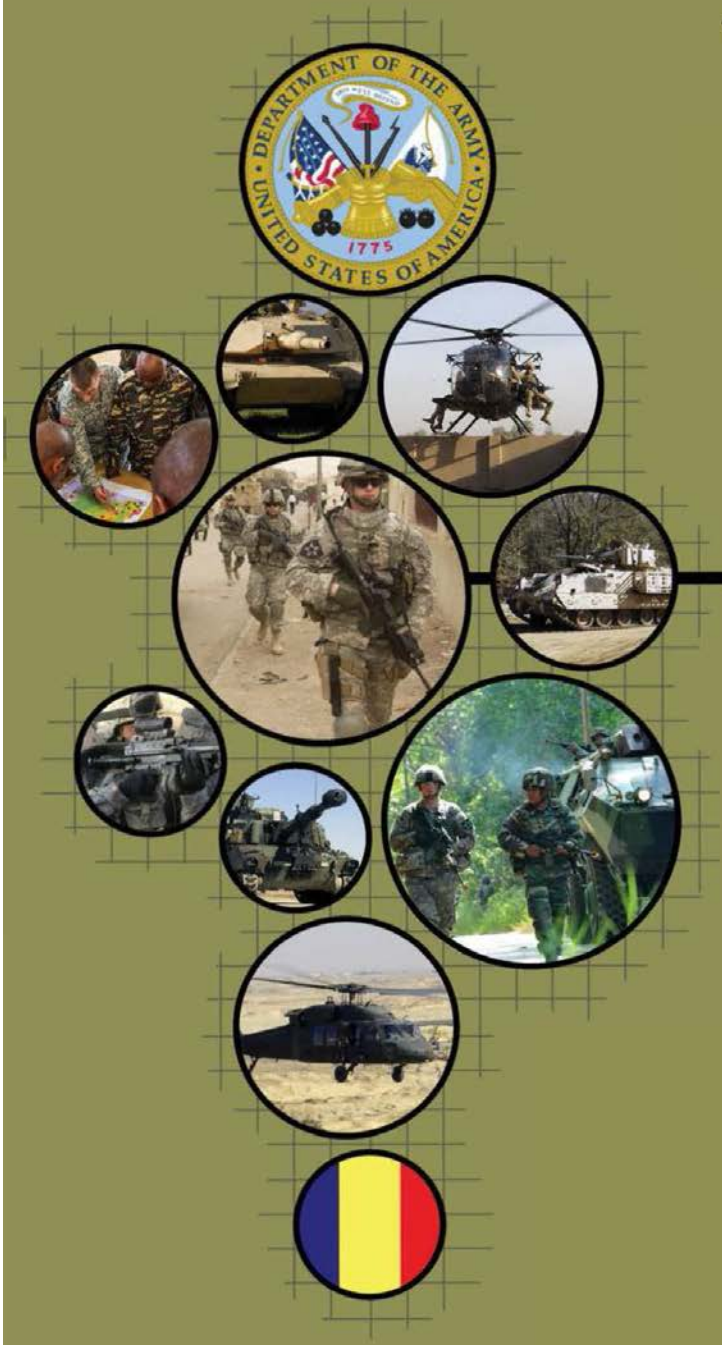
TRADOC Pamphlet 525-8-6



The U.S. Army Concept for

Cyberspace and Electronic Warfare Operations

2025-2040

January 2018

This page intentionally left blank

From the Director
United States (U.S.) Army Capabilities Integration Center

The U.S. Army is the Nation's principal land force organized, trained, and equipped for prompt and sustained combat on land. Today's adversaries have studied how the U.S. Joint Force prefers to operate and have adapted by developing capabilities that contest U.S. operations on land, at sea, in the air, in space, and in cyberspace, as well as across the electromagnetic spectrum, information environment, and cognitive dimension of warfare. Defeating future enemies that possess advanced capabilities calls for land forces operating as part of integrated joint teams that conduct simultaneous and sequential operations across multiple domains. In Multi-Domain Battle, future Army forces will fight and win across all contested spaces to create windows of advantage across multiple domains that enable Joint Force freedom of action to seize, retain, and exploit the initiative.

TRADOC Pamphlet 525-8-6, *The U.S. Army Concept for Cyberspace and Electronic Warfare Operations* expands on the ideas presented in TRADOC Pamphlet 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World (AOC).* This document describes how the Army will operate in and through cyberspace and the electromagnetic spectrum and will fully integrate cyberspace, electronic warfare (EW), and electromagnetic spectrum operations as part of joint combined arms operations to meet future operational environment challenges. Cyberspace and EW operations provide commanders the ability to conduct simultaneous, linked maneuver in and through multiple domains, and to engage adversaries and populations where they live and operate. Cyberspace and EW operations provide commanders a full range of physical and virtual, as well as kinetic and non-kinetic, capabilities tailored into combinations that enhance the combat power of maneuver elements conducting joint combined operations.

This concept serves as a foundation for developing future cyberspace and electronic warfare capabilities and helps Army leaders think clearly about future armed conflict, learn about the future through the Army's campaign of learning, analyze future capability gaps and identify opportunities, and implement interim solutions to improve current and future force combat effectiveness.

ROBERT M. DYESS, JR.
Major General, U.S. Army
Acting Director, Army Capabilities
Integration Center

This page intentionally left blank

Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Eustis, Virginia 23604

***TRADOC Pamphlet 525-8-6**

9 January 2018

Military Operations

THE U.S. ARMY CONCEPT FOR CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS

FOR THE COMMANDER:

OFFICIAL:

SEAN B. MacFARLAND
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff

RICHARD A. DAVIS
Senior Executive
Deputy Chief of Staff, G-6

History. This pamphlet is a new United States Army Training and Doctrine Command (TRADOC) 525-series pamphlet commissioned by the Director, Army Capabilities Integration Center (ARCIC).

Summary. This pamphlet describes how the Army will operate in and through cyberspace and the electromagnetic spectrum and integrate cyberspace operations, electronic warfare, and electromagnetic spectrum operations fully into joint combined arms operations to meet future operational environment 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 reference for war games, experimentation, and innovation aimed at maintaining the U.S. Army as the preeminent ground force in the world.

*This pamphlet supersedes TRADOC Pamphlet 525-7-6 dated 16 Aug 2007 and TRADOC Pamphlet 525-7-16 dated 28 Dec 2007.

Proponent and exception authority. The proponent of this pamphlet is the TRADOC Headquarters, Director, ARCIC. 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, ARCIC (ATFC-ED) 950 Jefferson Ave, Fort Eustis, VA 23604-5763.

Suggested improvements. Submit comments and suggested improvements via the Army Suggestion Program online at https://armysuggestions.army.mil (Army Knowledge Online account required) or via DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Director, ARCIC (ATFC-ED), 950 Jefferson Ave, Fort Eustis, VA 23604-5763.

Availability. This publication is only available on the TRADOC Administrative Publications website at http://adminpubs.tradoc.army.mil/

Summary of Change

TRADOC Pamphlet 525-8-6
The U.S. Army Concept for Cyberspace and Electronic Warfare Operations

This new pamphlet, dated 9 January 2018-

o Consolidates and updates guidance for the conduct and integration of cyberspace, electronic warfare, and spectrum management operations into joint combined arms operations.

o Provides applications and ideas for conducting cyberspace and electronic warfare operations in a holistic, synchronized, and integrated manner to create and exploit windows of advantage in or across multiple domains, the electromagnetic spectrum, and information environment.

o Identifies required capabilities and science and technology enablers necessary to implement the ideas in this concept.

Content

This page intentionally left blank

Chapter 1
Introduction

1-1. Purpose

a. United States (U.S.) Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-8-6, The U.S. Army Concept for Cyberspace and Electronic Warfare Operations (2025-2040), addresses applications and ideas for the conduct and integration of cyberspace, electronic warfare (EW), and spectrum management operations (SMO) into joint combined arms operations. The ability to employ cyberspace, EW, and SMO capabilities as an integrated system, acting as a force multiplier, improves the commander's ability to achieve desired operational effects. Cyberspace 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 capabilities in support of joint combined arms operations across multiple domains. Cyberspace, EW, and SMO link inextricably and support operations in a complimentary manner.

b. Cyberspace and EW operations are essential to the conduct of joint combined arms operations. While these activities differ in their employment and tactics, their functions and capabilities must integrate and synchronize to maximize their support. Cyberspace operations include Department of Defense (DOD) information network (DODIN) operations, defensive cyberspace operations (DCO) and offensive cyberspace operations, while electromagnetic spectrum (EMS) operations (EMSO) holistically includes all aspects of EW and SMO.[1] EW consists of Electronic Attack (EA), Electronic Protect (EP), and Electronic Support (ES). When discussing the DODIN, this concept will address the Army's portion of the DODIN as DODIN-Army (DODIN-A).

c. This concept expands on the ideas in joint and Army concepts, insights from joint and Army war games, Network Integration Evaluations, Army Warfighting Assessments, experiments, and studies. It provides a conceptual basis for future capabilities based assessments and capabilities development. The end state is for Army forces to have fully capable cyberspace and EW capabilities and the authorities to conduct effective cyberspace operations as part of their overall combined arms strategy to support joint combined arms operations. Cyberspace and EW operations provide the commander the capability to process and manage operationally relevant activities across multiple domains, both physical and virtual. Cyberspace and EW operations provide commanders the ability to conduct simultaneous, linked maneuver in and through multiple domains, and engage adversaries and populations where they live and operate. Cyberspace and EW operations provide commanders a full range of physical and virtual, as well as, kinetic and non-kinetic capabilities tailored into combinations that enhance the combat power of maneuver elements conducting joint combined operations.

d. Focus areas for this concept.

(1) This concept proposes a future vision and capability requirements that address how cyberspace and EW operations will enhance the Army's ability to fight and win in a complex world. This document identifies challenges and opportunities presented by the cyberspace domain and the EMS when conducting multi-domain operations.

(2) This document describes how the Army will conduct cyberspace and EW operations as a part of combined arms operations with joint, interorganizational, and multinational partners to support mission requirements. This concept proposes a combined arms team approach as the conceptual foundation for the Army's future conduct of cyberspace operations. This approach employs organic and expeditionary cyberspace and EW operations augmentation forces and capabilities from and into numerous locations and domains, presenting multiple dilemmas to an enemy, limiting enemy options, while avoiding their strengths.

(3) This concept identifies required capabilities for conducting cyberspace and EW operations as part of joint combined arms operations in support of Multi-Domain Battle.[2]

(4) This concept also discusses how Army forces make cyberspace and EW operations a fundamental and habitual component of its leader development and education, as well as individual and collective training efforts. This concept also identifies how the Army produces and maintains a highly capable and skilled cyberspace workforce.

(5) Finally, because technology, dependencies, threats, and vulnerabilities will change rapidly, this concept does not deliver a definitive solution to conducting actions in and through the cyberspace domain and EMS that result in the accomplishment of commander's objectives. Rather, it describes how the Army provides foundational capabilities to commanders and staffs to enable integrated cyberspace operations that enhance the combat power of Army forces.

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

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

1-4. Background

a. In 2013, the J-5 published Joint Publication (JP) 3-12, *Cyberspace Operations*, establishing a common taxonomy and lexicon for cyberspace operations. In December 2013, the U.S. Army approved the Army cyberspace operations capabilities based assessment, which supported numerous capabilities development efforts spanning doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P).

b. In 2014 the Army officially established the Army Cyber Institute and the U.S. Army Cyber Center of Excellence. In 2015, the Army created the Army Leaders Cyberspace Operations course and integrated it into intermediate level education, home station training, and cyber pilot events to benefit operational army units. Recently, the Army launched the Cyber Support to Corps and Below study initiative designed to provide tactical commanders with integrated cyberspace operations, EW, intelligence, and information operations (IO) capabilities, and to develop, and implement the necessary DOTMLPF-P changes required for integrating cyberspace operations, EW, intelligence, Fires, and IO.

c. In 2017, the Army published Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, establishing roles and responsibilities for commanders and staffs, and providing impetus to revise Army doctrine to incorporate cyberspace and EW operations language and operational considerations.

d. In the context of the emerging multi-domain battle concept, the ability to integrate cyberspace, intelligence, space, and IO will be critical to operational success. This integration, especially at the tactical level, will ensure commander's access to cross-domain combined arms capabilities for both mounted and dismounted operations. Cyberspace and EW cross-domain capabilities also give commanders multiple options while presenting multiple, simultaneous dilemmas to an adversary. Communication capabilities, as a function of cyberspace operations, support multifunctional battle teams conducting disaggregated maneuver. The offensive and defensive capabilities of cyberspace operations, in conjunction with critical communications capabilities, will be central to aggregate sufficient combat power within time and space successfully to defeat enemy elements. Cyberspace capabilities are key enablers of multi-domain battle.

e. The complex nature of the cyberspace and EW operations environment, combined with the demands of multi-domain battle, have made it necessary to create an updated cyberspace operations concept based on a more mature understanding of the cyberspace domain, the EMS, and the operations within them as elements of combined arms.

1-5. Assumptions

a. The assumptions from TP 525-3-0, Army Capstone Concept (ACC) and TP 525-3-1, Army Operating Concept (AOC) apply to this concept.

b. The following assumptions also apply.

(1) Operations in cyberspace and the EMS will be more complex and have greater impact on other domains as political, economic, informational, and cultural systems become more interconnected and the domain becomes more congested with military and commercial users.

(2) The EMS will be more contested and congested. An increasing amount of network and data transmissions will be wireless, taking place via the transmission of electromagnetic energy contributing to an enormous expansion of the potential target sets and potential vulnerabilities.

(3) Advancements in commercially available dual-use technologies and software defined systems drive future threat diversity and complexity.

(4) Joint cyber mission forces will be fully manned and ready to meet the Nation's and Combatant Command's operational needs.[3]

(5) Army units possess the authorities, through Combatant Commanders, to approve or conduct all aspects of cyberspace operations in support of joint combined arms operations per applicable execution orders and rules of engagement.[4]

(6) The DOD will implement the joint information environment[5] providing a standardized functional and technical framework that is responsive to both strategic and tactical operational needs.[6]

(7) Army units will need to operate with joint, interorganizational, and multinational partners to conduct strategic and operational movement, reconnaissance, and security operations, joint combined arms maneuver, and wide area security.

(8) The Army will rely on a single converged DODIN-A transport backbone.

(9) Army forces will operate in a degraded cyberspace environment.

1-6. Linkage to the Army Concept Framework

a. TP 525-8-6 is a leadership-directed concept, not an Army functional concept. Although cyberspace operations are not presented as a warfighting function, cyberspace operations are cross-cutting and integral to all joint functions and Army warfighting functions.

b. This concept is consistent with the ACC, which states that the Army requires a full range of cyberspace and EMS capabilities to provide commanders the ability to adapt to rapidly changing missions, conduct decentralized operations over wide areas, maintain operational freedom of maneuver, exercise mission command, and gain and maintain the initiative in cyberspace.

c. This concept expounds on the AOC regarding cyberspace operations. The AOC describes the Army's contribution to globally integrated operations and addresses the need for Army forces to provide foundational capabilities for the Joint Force and to project power from land into other domains. This document also addresses the relationship of cyberspace capabilities to operational considerations, activities and capabilities in other domains.

Chapter 2
Operational Environment

2-1. Future operational environment

a. The future operational environment (OE) is outlined in the *Joint Operating Environment 2035* [7], *Joint Cyberspace Concept*, *Joint Concept for Electromagnetic Spectrum Operations*, the ACC, and the AOC.[8] These concepts describe a future OE where adversaries will employ a combination of tactics and technologies that enable them to overcome or avoid U.S. military strengths and exploit perceived weaknesses.[9] The future OE will be more unpredictable, complex, and potentially dangerous than today.[10] In the future, the physical structure of cyberspace will be extremely vulnerable to attack by an array of destructive weapons, including high-power microwave munitions and laser systems which are increasingly effective against digitized, miniaturized, and integrated circuits.[11] Because these challenges and changes can occur swiftly, the Army must adopt advanced cyberspace operations capabilities at a more rapid rate than current capability development timelines even while in a constrained fiscal environment.

b. State and non-state actors will 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 positioning system jammers and radio-frequency weapons that utilize the EMS to exploit Army reliance on technology.[12]

c. Threats manifest themselves in combinations of national governments, terrorists, organized crime groups, hacktivists, hackers, bot-network operators, foreign intelligence services, insiders, phishers, spammers, spyware and malware authors.[13] 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 that enable 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 to U.S. operations.

d. Continued urbanization and widespread access to social media will increase operational complexity. Army Soldiers, leaders and commanders may become overwhelmed with information and face multiple dilemmas, across multiple operational domains, in shorter periods. The increase in overall operational complexity will require Army personnel to perform their duties with greater skill and understanding of cyberspace, the EMS, and the OE.[14]

e. Taken in total, these threats pose a significant challenge to the Army’s ability to conduct joint operations. Section 2-2 frames the threat within the cyberspace domain while 2-3 further refines the threat environment within the context of the EMS.

2-2. The cyberspace domain

a. An accessible and contested cyberspace domain exacerbates the uncertainty of future war. More adversaries will gain access to cyberspace capabilities enabling them to fight across multiple domains simultaneously.[15] In the future, the Army will see an increase in the number of "smart" devices and sensors connected to the DODIN-A. Since every device presents a potential vulnerability, this trend represents an exponential growth of targets through which an adversary could access Army operational networks, systems, and information. Conversely, it presents opportunities for the enhanced synchronization of Army technologies and information to exploit adversary dependencies on cyberspace.[16] Difficulty and untimely attribution of attacks in cyberspace, as well as the legal ambiguities of attacks in cyberspace, will complicate reactions to attacks both inside and outside of cyberspace.

b. Adversaries will conduct complex cyberspace attacks integrated with military operations or independent of traditional military operations. They will attempt to avoid U.S. strengths (such as long-range surveillance and precision fires) through traditional countermeasures such as dispersion, concealment, and intermingling with civilian populations.[17] As military technologies transfer more easily, potential threats will emulate U.S. military capabilities to counter U.S. power projection and limit U.S. freedom of action.[18]

c. State and non-state actors will apply technologies to disrupt U.S. advantages in communications, long-range precision fires, and surveillance.[19] Adversaries will operate outside of the geographical area of operations to infiltrate Army and partner systems.[20] In many cases, adversaries will use cyberspace to attack Army forces simultaneously in multiple areas of operation to include the homeland.[21]

d. The spread of mobile technologies, especially in developing nations, will dramatically increase the number of people able to access and share information rapidly. Adversaries conduct sophisticated influence operations and leverage cyberspace as a force multiplier in the information environment. They use propaganda and disinformation through social media to affect public perception, sway public opinion, and catalyze protests and violence in ways that popular movements once took months or years to build. Cyberspace also provides adversaries an effective and inexpensive means for recruitment, propaganda, training, command, and control.

e. 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 decisions for themselves on the battlefield using advanced algorithms and artificial intelligence. Consequently, that decision-making algorithm may be hijacked and the artificial intelligence corrupted, posing a danger to Army forces and technologies. Because of the proliferation of autonomous systems, fail-safe technologies and software are required to maintain positive control.[22]

f. Army forces use cyberspace operations to understand and develop influence in the human dimension.[23] Cyberspace operations offer access, placement, and influence to multiple domains which may allow better positioning of Army forces to conduct cross-domain operations while also enabling a means of persistent engagement over distance.[24]

2-3. Electronic warfare (EW) and the electromagnetic spectrum (EMS)

a. Modern warfare is dependent on use of the EMS; therefore, the EMS is a central characteristic of the future operational environment. As operational dependence on the EMS has grown, so have adversaries' efforts to target this vulnerability. The expanding ability of current and future adversaries to sense and observe electromagnetic signatures in the EMS is a reality in an evolving and increasingly complex operational environment. Adversaries are also growing reliant on the EMS, creating both vulnerabilities and opportunities for Joint Force exploitation.[25]

b. The EMS is becoming more congested and contested as commercial users, adversaries, partners, and the U.S. military compete for available bandwidth. Use of EMS and EMS-enabled capabilities to achieve effects may reduce risk by limiting exposure of combatants, lower costs by offering significant life-cycle savings over conventional munitions, and present commanders with an array of non-kinetic options that can achieve effects unattainable through kinetic fires.[26]

c. Army forces cannot assume unhindered access to the cyberspace domain and EMS. Physics, technology, governing policy, and demand for bandwidth all contribute to congestion of the EMS while reducing its availability for military use. Adversary EW capabilities also have the potential to severely impact operational use of the EMS. Current Army forces have operated under the

assumption that they will possess cyberspace and EMS superiority, however, peer and near-peer adversaries have demonstrated the ability to challenge this assumption.

d. Many EMS innovations are dual-use (civilian and military applications) systems capable of directly challenging what was once an exclusive military niche, potentially allowing adversaries to achieve parity with U.S. capabilities.[27] Furthermore, the U.S. uses inexpensive Federal Communication Commission-compliant and Internet protocol-based communication technologies in many of its combat systems. This use of standardized international operating attributes and behaviors leaves U.S. systems vulnerable to common exploits.

e. Advanced materiel properties and switching architectures have increased the speed and capacity of EMS operations 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.[28] Technologies such as application-specific integrated circuits, programmable logic devices, digital radio frequency memory, and shared aperture electronic attack, increase the number of ways users can attack through the EMS. Lower-power demand, smaller size and weight, higher sensitivity, and wider frequency ranges for sensing and transmitting revolutionize a commander's operational capabilities. These technological advances expand access to the EMS resulting in congestion from commercial users, local and national host nation governments, adversaries, partners, and Army EMS-enabled systems that saturate available bandwidth and constrain maneuver within the EMS.

f. The shrinking size and power requirements of many EMS systems and architectures makes them more suitable for employment by remote, robotic, and autonomous systems, including artillery and rocket EW munitions, dramatically expanding the commander's potential to conduct EMS operations with small signature platforms and minimal risk to Army forces. They also reduce risk to non-combatants on the battlefield by limiting property destruction and loss of life, which aid the Army in wide area security core competency.

g. Threats to the EMS affect the Army whether at home station or deployed. 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 just as effective in denying Army use of the EMS, and in some cases, more of a detriment to operations. In addition, organized cybercrime has now eclipsed the world-wide drug-trade enterprise in gross profits and reach. These threats pose a serious concern to U.S. domestic industries and governments will be more significant for Army forces when responding to homeland support requirements.

Chapter 3
Military Problem, and Solution Components

3-1. The military problem
How does the Army, in conjunction with unified action partners, provide critical cyberspace and EW operations capabilities, in support of joint combined arms operations, conducted across multiple domains, while simultaneously denying the same to adversaries?

3-2. Central idea

a. The Army conducts cyberspace and EW operations in a holistic, synchronized, and integrated manner to exploit temporary windows of advantage to achieve positions of advantage in or across multiple domains, the EMS, and information environment to seize, retain, and exploit the initiative to defeat the enemy. Army forces conduct operations across the cyberspace domain and the EMS with other elements of combined power to achieve commander's objectives. Cyberspace and EW operations capabilities provide ground combat forces with cross-domain capabilities at the tactical level and support the employment of optimized manned-unmanned combined arms teams for both mounted and dismounted operations. The Army incorporates cyberspace and EW operations as a fundamental and habitual component of its leader development and education, and its individual and collective training efforts to produce and maintain a highly capable military and civilian cyberspace workforce. The Army recruits, trains, and retains skilled cyberspace and EW operations personnel.

b. Cyberspace and EW operations support commanders in the conduct of joint combined arms operations by integrating cyberspace, EW, and SMO under the concept of cyberspace operations. This single cyberspace operations concept shapes, or can be shaped, by available capabilities to enable Multi-Domain Battle in operational environments. An example of these shaping attributes resides in the convergence of cyberspace operations, information operations, and space operations to project power outward from land into other domains and to ensure freedom of maneuver and action.

c. The intent of cyberspace and EW operations is to be specific enough to provide the right effects, but broad enough to minimize constraint on the types of supporting capabilities that generate those effects regardless of origin. Cyberspace and EW operations are aided in generating effects through reliance on a converged single transport backbone that enables a baseline cyberspace capability.

d. Cyberspace and EW operations provide capabilities that support the operation of multifunctional battle teams that sense, close with, and destroy enemy elements, influence populations, and seize and occupy terrain. Cyberspace and EW operations facilitate disaggregated maneuver in conjunction with mission partners across cyberspace, the EMS, the information environment, and the cognitive dimension of warfare.

3-3. Solution synopsis

a. Army Forces conduct a full range of cyberspace and EW operations, enabling commanders to achieve desired effects in multi-domain operations. Cyberspace and EW operations provide ground combat forces with cross-domain capabilities at the tactical level and enable the employment of optimized manned-unmanned combined arms teams for both mounted and dismounted operations. Cyberspace and EW operations support multifunctional battle teams conducting disaggregated maneuver while also enhancing the ability to aggregate sufficient combat power within time and space to defeat enemy elements. Army forces have the capability to detect enemy signatures across the spectrum enabling quick and accurate situational understanding to enable rapid action to exploit temporary windows of superiority across multiple domains. Cyberspace and EW operations support identification of seams in enemy defenses through enhancing the continuous fusion of reconnaissance in the physical and virtual layers of cyberspace to sequence actions in a manner to capitalize on rapidly changing conditions.

b. Cyberspace and EW operations are joint in nature. The Army uses cyberspace and EW capabilities to integrate mission partners across space, the EMS, the information environment, and the cognitive dimension of warfare to outmaneuver enemies physically and cognitively. Throughout the continuum of operations, planning and coordination between the appropriate staff sections is critical to ensure situational understanding; rapid employment of tailored cyberspace operations forces; production and dissemination of intelligence, and the delivery of cyberspace effects.

c. Fully integrated cyberspace and EW operations capabilities at echelon provide organic capabilities to support maneuver forces including formations engaged in semi-independent operations, while also providing pooled capabilities that can offer remote support and augmentation to tactical organizations. These capabilities integrate into existing force structure models and enable supported organizations to conduct all aspects of cyberspace and EW operations.[29] Organic cyberspace and EMS sensors, EW attack and jammer capabilities, and automated electromagnetic battle management capabilities allow tactical formations to attack or jam enemy systems while minimizing friendly systems' vulnerabilities. Globally tailored cyberspace mission forces enhance a commander's ability to maneuver by creating denial effects from sanctuary or close to the fight.

d. Army units use requisite authorities and preapproved actions through the combatant commander to create cyberspace and EW effects in their areas of operations. Title 10, United States Code provides authorities and establishes roles to staff, train, and equip forces for military operations in cyberspace. This structure supports the fielding of select, organic cyberspace operations capabilities, while legal and policy considerations often constrain cyberspace authorities provided under Title 50 at the combatant command level.

e. The Army develops a highly-trained cyberspace and EW workforce where individual and collective training and education enables cyberspace personnel to conduct cyberspace and EW operations as an indispensable imperative to mission success.

f. 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 and the EMS to meet the commander's objectives. Commanders employ cyberspace and EW operations capabilities to deceive, degrade, disrupt, deny, destroy, or manipulate across multiple domains. These capabilities exploit adversary systems to facilitate intelligence collection, target adversary cyberspace and EMS functions, and create first order effects. 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, applying combined arms in and across all domains.

g. Army Forces must think globally, and act locally, in the cyberspace domain to shape the physical and virtual behavior of humans and their devices to gain opportunity and advantage. This requires commanders to understand 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 these operations. It also requires understanding that threat activities 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 ground combat forces to exploit enemy vulnerabilities, seize and retain key terrain, and hold targets at risk for sustainable outcomes. Army forces use cyberspace capabilities to exploit psychological, technological, temporal and spatial advantages over the adversary. Cyberspace capabilities enable combined arms teams to converge intelligence, reconnaissance, movement, and fires information to create windows of advantage. Cyberspace and EW operations capabilities ensure the Army prevails by integrating into the targeting process, facilitating the synchronization and integration of multiple elements of combat power to gain an advantage, protect that advantage, and place adversaries at a disadvantage.

h. Commanders rely on a common operational picture that identifies cyberspace and EW opportunities, risks, and vulnerabilities. Situational understanding, as it relates to cyberspace and EW operations, provides a visual representation of the entire cyberspace and EMS environments that supports the battle rhythm and command decision cycle. The common operational picture provides indications and warnings that enable commanders to act, react, and counteract at speed while conducting offensive and defensive operations simultaneously.

i. The DODIN-A is an integral part of cyberspace and EW operations. It serves as an operational warfighting platform that enables global collaboration, ensures access at the point of need, extends to the tactical edge, and can enable the full range of available cyberspace and EW options. The DODIN-A enables maneuver from a strategic distance, using Army operational and institutional force capabilities to prevent conflict, shape outcomes, and ultimately win. DODIN-A capabilities allow Army forces to operate more dispersed over wider areas in support of joint combined arms operations. The convergence of disparate DODIN-A transport capabilities into a single transport backbone is a crucial component of operationalizing cyberspace.

j. Cyberspace defense of the DODIN-A provides threat monitoring, detection, analysis, and response actions. Army systems provide autonomous detection and response capabilities. By building, operating, and defending cyberspace infrastructure, cyberspace operations forces enable commanders to conduct decentralized operations, enhance understanding of the operational

environment, and transition rapidly between operations. A defended and resilient DODIN-A is essential in establishing and supporting multifunctional battle teams conducting disaggregated maneuver.

k. Army cyberspace and EW operations provide synchronization and integration of cyberspace and EW into the intelligence, planning, and targeting processes to achieve required cyberspace effects. Cyberspace enabled cross-domain and counter-fire sensors improve commander's situational understanding, and support suppression or destruction of enemy fires systems. Authorities required for approval of cyberspace effects are clear, and an efficient approval process allows commanders to seize opportunities, and produce cyberspace effects at the time and place of their choosing to achieve localized effects by extending cyberspace capabilities to the tactical edge. Cyberspace and EW operations provide effects as part of an integrated fire support plan, while also assisting in combat assessment.

l. The Army counters cyberspace and EW threats, mitigates degraded access to cyberspace and the EMS, and takes local actions against enemy cyber electromagnetic capabilities to achieve local effects.[30] Army forces detect and disrupt adversaries' cyberspace enabled operations while effectively performing emissions control and other means of signature management. Mission command systems provide external connectivity to global support networks; however, units are not dependent on continuous connectivity to fight. Army forces possess the ability to operate with degraded or denied access to cyberspace, space, and the EMS. Army forces coordinate their efforts across all domains, the EMS, interorganizational partners, and allies.[31]

m. To achieve full integration of cyberspace, EW, and SMO, cyberspace operations requires advanced detection, characterization, presentation capabilities, and adaptive EMS systems. Cyberspace and EW operations provide commanders the ability to conduct operations in and through the EMS at a time and place of their choosing, while avoiding electromagnetic detection. Minimizing or masking system signatures and using concealment, deception, and advanced decoy systems which can replicate multiple signatures including thermal and radio frequency confuse enemy targeting.

n. Cyberspace and EW operations provide capabilities that enhance the impact to potential adversaries in both the physical dimension and cognitive functions creating multiple dilemmas. The Army uses cyberspace and EW capabilities to support information warfare. Information warfare fully encompasses and broadens current information operations and spans several capabilities and functions such as: military information support operations, military deception, operations security, EW, physical attack, special technical operations, information assurance, DODIN-A operations, public affairs, and civil-military operations.

o. Army forces incorporate cyberspace and EW operations as fundamental and habitual components of its leader development, education and training effort to produce and maintain a highly capable military and civilian cyberspace operations workforce. The scope of cyberspace operations leader development, education, and training will change across all ranks, positions, and organizational command structures. The Army uses a common baseline of training for personnel to reduce risk posed by the weakest link in cybersecurity, the user.

p. The Army unit training construct builds on individual Soldier and leader cognitive, interpersonal, cultural, and technical skills developed in the institutional learning environment. The Army achieves realistic training environments in cyberspace and the EMS by providing complex and challenging collective unit training opportunities that transform individual adaptive skills into adaptive collective skills that strengthen unit readiness. To be adaptive, the unit cyberspace training environment is responsive to commanders' and leaders' training programs; it will be scalable and tailored, and capable of quickly adjusting to a changing operational environment marked by a contested cyberspace domain. The future training construct achieves adaptive training in new and markedly different ways from how the Army trains today through the integration of training environments, leveraging technology, and innovative management of training support to meet commanders' and leaders' training requirements.[32]

q. The Army invests significantly in the human dimension to recruit, train, and develop technologically capable people for the cyberspace and EW workforce. Assessments that identify technical aptitude will assist the Army in putting the right people onto the best professional development path, and it will help shape and direct individual training and education.

r. Acquisition practices are reformed to acquire critical cyberspace technologies rapidly.[33] In their current forms, the Joint Capabilities Integration and Development System process and Army capabilities development processes, described in TRADOC Regulation 71-20, do not afford the speed and flexibility the Army requires to innovate, develop, and field capabilities for cyberspace operations.[34] To be more responsive, the Army must also improve basic research, applied research, and advanced technology development and the ability to rapidly transition these into fielded solutions to support cyberspace operations.

s. The Army balances near-term requirements with future development investments to support innovation. Army leaders assess what is possible and prioritize promising technologies.[35] The research and development communities apply an analytical framework to select candidate technologies that have potential to address warfighting challenges and capability gaps.[36] Testing and analysis includes predictive modeling. As technological innovation speeds, it becomes harder for a centrally planned acquisition system to keep up and stay ahead. Army leadership will recommend changes to policy and U.S. code to ensure access to advanced technology.[37]

3-4. Supporting ideas

a. Successful operations in the cyberspace domain require very specific expertise in information theory, computer science, and related sciences, and then applying this expertise to military tactics, operations, and strategy. Providing this expertise requires a highly skilled and trained military and civilian workforce that places a premium on analytical skills and critical thinking. Army recruitment and retention activities identify opportunities to grow the cyberspace talent pool, promote cybersecurity education, and develop a strong cybersecurity career field. Providing the support to achieve this institutional Army foundation for cyberspace and EW operations produces a resilient, protected, multi-tiered, and rapidly configurable network. This network enables an information advantage in support of Army and joint combined operations, supports Soldier requirements, and is responsive to commanders throughout all phases of operations in all operational environments.

b. The Army adapts and expands the current, learner-centric Army learning model and its continuously adaptive learning approach.[38] The future career-long continuum integrates unit training, military education, self-development, and experience into a holistic learning approach that synchronizes with Army talent management.

c. Cyberspace and EW operations support all warfighting functions and facilitate joint combined arms operations. 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.

d. Operational cyberspace.

(1) Offensive cyberspace operations project power by applying force in and through cyberspace to deny and manipulate the adversary's access to the cyberspace domain. Army forces mass effects, by employing kinetic and non-kinetic actions, leveraging all capabilities available to gain advantages in cyberspace and the EMS in support of commander's objectives. Cyberspace operations generate and exert combat power in and through cyberspace as part of a combined arms team. Effects delivered from cyberspace can be both kinetic and non-kinetic, and can span all domains based on the commander's intent. Army cyberspace operations leaders, staffs, formations, elements and teams, spanning all echelons, enable freedom of maneuver and action in the cyberspace domain, and deliver decisive cyberspace effects during joint combined arms operations.

(2) DCO consists of activities to protect against, detect, characterize, counter, and mitigate cyberspace threat events generated by adversary cyberspace operations. DCO are intended to defend DOD or other friendly networks. DCO preserves the ability to utilize friendly force cyberspace capabilities passively and actively while protecting data, networks, and other designated systems.

(3) DODIN-A operations consist of actions taken to design, build, configure, secure, operate, maintain, and sustain communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, user/entity authentication, and non-repudiation. The DODIN-A is the baseline cyberspace platform for Army operations. DODIN-A operations include proactive measures such as configuration control, patching, information assurance measures and training, physical security, secure architecture design, operation of host-based security systems and firewalls, and encryption of data.

(4) EW is any military action involving the use of electromagnetic and directed energy to control the EMS or to attack the enemy. EW consists of three functions: electronic attack, electronic protection, and electronic warfare support. (These functions are referred to as divisions in joint doctrine.)[39]

(5) Intelligence, surveillance, and reconnaissance include activities in cyberspace conducted to gather intelligence from target and adversary systems that may be required to support future

operations. Intelligence, surveillance, and reconnaissance 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.

(6) Operational preparation of the environment in support of cyberspace and EW operations consists of predictive analysis used in conjunction with intelligence and non-intelligence enabling activities, conducted to plan and prepare for potential follow-on military operations. Army cyberspace and EW forces will use operational preparation of the environment to gain and maintain access to systems and processes, and to position capabilities to facilitate follow-on actions. This operational preparation of the environment will include identifying data, software, system and network configurations, or physical structures connected to, or associated with, the network for the purposes of determining system vulnerabilities; and actions taken to assure future access and/or control of the system, network, or data during anticipated hostilities.

(7) Situational understanding in cyberspace is the requisite current and predictive knowledge of cyberspace and the OE upon which cyberspace operations depend, including all factors affecting friendly and adversary cyberspace forces. Improved cyberspace situational understanding enables informed decision-making at all levels, through flexible and focused products and processes.

e. Operational EMSO.

(1) EMSO represents a distinct enduring capability to provide Army commanders an advantage within the EMS. EMSO provides the commander with the means to achieve desired effects in cyberspace through the EMS. Because EMS links and wireless infrastructure comprise part of the physical network layer of cyberspace, Army EMSO capabilities will be essential to the successful operation of the DODIN-A, associated sensors, as well as unmanned ground and aerial platforms.

(2) Commanders rely on freedom of maneuver in the highly contested and congested EMS to realize the full potential of Soldiers and systems. Army forces have the capacity to see, understand, operate in, and defend the EMS in all phases of operations.

(3) The ability to integrate and direct EMS-enabled assets at all levels of command is critical to effective operations. Electronic attack and use of directed energy require integration within the staff planning process across all warfighting functions. Use of the EMS for communications requires prioritizing and coordinating with other users to optimize bandwidth usage. EW support and signals intelligence monitoring synchronize to maximize effective and efficient use of limited assets.[40]

(4) Commanders protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability.

(5) The Army uses cyberspace and EW operations capabilities to plan and manage use of the EMS and combat the strengths, and exploit vulnerabilities, of an evolving range of threat EW capabilities. These actions deny opponents an actual or perceived advantage in the EMS and support freedom of action and positions of advantage across the EMS. Army cyberspace

operations capabilities sense, intercept, identify, locate, and distinguish between the sources of intentional, and unintentional radiated electromagnetic energy with increased precision. Army forces use electromagnetic energy, directed-energy, and anti-radiation weapons to attack the enemy, while simultaneously protecting Soldiers, facilities, and equipment from adverse effects of enemy use of the EMS.

f. Expanded cyberspace operations authorities gained through strong policy guidance.

(1) Many effects of cyberspace operations require considerable legal and policy review. This review often creates lengthy lead times during the planning and preparation phases, even though the effects may occur nearly instantaneously once executed. The Army uses the appropriate policy and authorities to coordinate with other agencies to conduct actions in and through cyberspace and the EMS.

(2) Army forces use policies that address the cyberspace domain holistically to successfully support joint combined arms operations. The Army possesses clear authorities and policies to deter, prevent, detect, defend against, respond to, and remediate hostile actions in cyberspace. The authorities and rules of engagement for cyberspace operations will continue to evolve, this evolution will continue to accelerate as the understanding of the cyberspace domain continues to mature.

g. Science and technology.

(1) Science, technology, and engineering shape the cyberspace operational environment, and drive cyberspace evolution. Private industry research and development are the catalyst for change in cyberspace. Gaining advantages in cyberspace and denying them to U.S. adversaries is achieved through futuristic, automated networks, which depend upon the same scientific knowledge base as that of the commercial technology environment. The Army leverages commercial innovation while also undertaking its own critical science and technology investments to develop cyberspace capabilities fully.

(2) Automated capabilities will provide commanders with improved situational understanding. These automated capabilities process a vast amount of data instantly, and then target adversaries to ensure they cannot seize the initiative effectively. Next generation analytics and decision support systems, with minimal operator interaction, enable the Army to build, operate, and defend its network while simultaneously defeating cyberspace attacks.

(3) Commanders employ fully automated cyberspace operations countermeasure systems to maintain freedom of action and initiative on the battlefield, and identify cyberspace events that degrade, disrupt, or destroy battlefield systems and networks. Army forces employ active defenses against malicious activities and support execution of counter offensive actions against aggressors in cyberspace.

(4) Army forces develop techniques to hide, mask or deceive adversary attempts to detect EMS signatures. Mitigating vulnerability requires developing more agile and redundant systems, employing passive sensors, and increasing position, navigation, and timing (PNT) assurance.

Improving reliance involves hardening of systems against EMS attack and building alternatives to a single point of failure.

(5) The Army employs more expeditionary cyberspace operations capabilities reducing the size, weight, and power of many cyberspace and EMS systems to make them more suitable for employment by remote, robotics, and autonomous systems. The Army deploys advanced antenna technology and dynamic spectrum access capabilities to increase efficient use of the available EMS.

h. Modeling and simulation.

(1) Army forces utilize state of the art modeling and simulation tools. Army forces gain efficiencies and increase training effectiveness through a balanced modeling and simulation training model supported by technological advances that reduce stovepipes. Simulations integrated into field exercises and gunnery create live, virtual, and constructive events that facilitate problem solving at the tactical edge. Army forces conduct training in garrison with support from state of the art cyberspace range capabilities that provide adaptable environments to develop and enhance both collective and individual skills.

(2) Advanced capabilities to collect, process, and disseminate information enables the Army to conduct more expeditionary cyberspace and EW operations capabilities. As the Army continues to utilize robotics in future operations effectively, these platforms equipped with more sensors, can enable dynamic spectrum access capabilities to increase efficient use of the available EMS. With these tools, data sets from the Internet of Things become both collectable and manageable. These capabilities can enable new methods to employ other functions such as counter intelligence or information operations.

Chapter 4
Conclusion

a. Success in the future operational environment requires the Army to conduct cyberspace and EW operations in a holistic, synchronized, and integrated manner to exploit temporary windows of advantage to achieve positions of advantage in or across domains, the EMS, and information environment to seize, retain, and exploit the initiative to defeat the enemy. To perform these actions, the Army staffs, equips, resources, trains, and sustains cyberspace and EW operations forces and organizes them into a mix of organic and pooled resources optimally positioned to support joint combined arms operations. The Army makes cyberspace and EW operations fundamental and habitual components of its leader development, education, and training effort to produce and maintain a highly capable military and civilian cyberspace and EW operations workforce. The Army changes personnel policies to recruit and retain skilled cyberspace and EW operations personnel.

b. This concept builds on existing Army DOTMLPF-P initiatives, while providing a realistic future vision (2025-2040). It is consistent with the *Joint Cyberspace Concept* and the Army Concept Framework, as well as other cyberspace related documents. This concept outlines

cyberspace and EW operations support to multi-domain battle which allows Army forces to outmaneuver adversaries physically and cognitively, applying combined arms in and across all domains. This concept serves as a starting point to inform ongoing cyberspace and EW operations and organization efforts within the Army.

c. The Army faces a complex and challenging environment where the expanding distribution of cyberspace and EMS technologies will continue to narrow the combat power advantage that the Army has had over potential adversaries. The proliferation of cyberspace weapons and EMS capabilities are a growing threat against a cyberspace dependent Army force that relies heavily on digital technologies. These future challenges require a full range of cyberspace and EW operations capabilities to provide commanders the ability to adapt to rapidly changing missions, conduct decentralized operations over wide areas, maintain operational freedom of maneuver, exercise mission command, and gain and maintain the initiative in cyberspace and the EMS during joint combined arms operations.

Appendix A
References

Section I
Required References.

For all references: ARs, DA PAMs, FMs, and DA forms are available at Army Publishing Directorate Home Page http://www.usapa.army.mil TRADOC publications and forms are available at TRADOC Administrative Publications at http://adminpubs.tradoc.army.mil Joint publications are available at http://www.dtic.mil

TP 525-3-1
The U.S. Army Operating Concept: Win in a Complex World

Section II
Related References

Capstone Concept for Joint Operations: Joint Force 2020.

Joint Cyberspace Concept

Joint Publication 3-0
Joint Operations

Joint Operating Environment 2035

Perkins, D. G. (2015, March). “Win in a complex world – but how?” *Army AL&T Magazine*, January – March 2015 pp 106-115. . Retrieved from http://usacac.army.mil/sites/default/files/documents/cact/GEN%20PERKINS%20HOW%20TO%20WIN%20IN%20COMPLEX%20WORLD.pdf

The U.S. Army Cloud-Enabled Network Concept of Operations

TP 71-20-3
The U.S. Army Training and Doctrine Command Concept Development Guide

TP 525-3-0
The U.S. Army Capstone Concept

TP 525-2-1
The U.S. Army Functional Concept for Intelligence

TP 525-3-3
The U.S. Army Functional Concept for Mission Command

TP 525-3-4
The U.S. Army Functional Concept for Fires

TP 525-3-6
The U.S. Army Functional Concept for Movement and Maneuver

TP 525-3-7
The U.S. Army Human Dimension Concept

TP 525-8-3
The U.S. Army Training Concept

USSTRATCOM, Operational Concept for Electromagnetic Battle Management.

Appendix B
Required Capabilities

B-1. Introduction
The TP 525-8-6 describes capabilities needed to execute the missions under the conditions described within this concept. The Army's ability to leverage cyberspace and cyberspace operations capabilities is critical to its operational success. Cyberspace operations capabilities will integrate fully with other capabilities at the commander's disposal to gain advantage, protect that advantage, and place adversaries at a disadvantage. Each required capability is followed by reference paragraphs from this concept, the AOC, and the ACC.

B-2. Cyberspace Operations RCs

a. A single Army information network that enables a regionally-engaged, globally-responsive, and multi-domain capable force. Future Army forces require a single, secure, and reliable network of command posts; air, ground, and waterborne platforms; dismounted leaders and Soldiers; and sensors linked by a tailorable suite of mission command applications, information services, and

communications infrastructure to enable expeditionary movement and maneuver, dispersion, decentralization, interoperability, collaboration, and uninterrupted mission command during joint combined arms operations (Army Functional Concept for Mission Command (AFC-MC): 3-4.c.(7) & F-2; AOC: 3-3.c., 3-3.e., 3-3.h., & 3-3.i.; and ACC: B-1.g.).

b. Fully integrated space and cyberspace electromagnetic operations to support multi-domain battle. Future Army forces require leaders, Soldiers, and Army Civilians who understand space, cyberspace, and electromagnetic spectrum capabilities, limitations, vulnerabilities, and interdependencies and who can integrate space and cyberspace electromagnetic operations to disrupt, degrade, or destroy enemy space and cyberspace electromagnetic capabilities and gain and maintain a technological advantage during joint combined arms operations (AFC-MC: 3-4.d.(1)& E-2.c.(4); AOC: 3-3.c.; ACC: B-1.c).

c. Advanced cyberspace capabilities to influence the behavior of people and machines. Future Army forces require the ability to build, operate, maintain, and defend friendly cyberspace, shape neutral cyberspace, and influence, attack, and exploit threat cyberspace to enable mission command and other network-based activities during joint combined arms operations (AFC-MC: 3-4.d.(3); AOC: 3-3h; and ACC: B-1.i., B-1.j., & B-1.k.).

d. A full complement of electronic warfare capabilities. Future Army forces require electronic warfare capabilities to gain or maintain advantage and freedom of action across all domains, and combat threats' strengths, exploit their vulnerabilities, and deny them advantage across the electromagnetic spectrum during joint combined arms operations (AFC-MC: 3-4.d.(4) and AOC: 3-3.h.).

e. Globally-networked and interoperable teams of joint, interorganizational, and multinational partners. Future Army forces require the ability to form and deploy rapidly multifunctional, globally-networked, and interoperable teams of Army forces and joint, interorganizational, and multinational partners that are responsive regionally to the combatant commanders' needs and the Army's institutional requirements across multiple domains and the range of military operations (AFC-MC: 3-4.c.(4); AOC: 3-3.a., 3-3.b., 3-3.d., & 3-3.g.; and ACC: B-7.c.).

Appendix C
Science and Technology

C-1. Technology application

a. Gaining, protecting, and exploiting the Army's cyberspace advantage is not easy. U.S. adversaries use the commercial marketplace as their combat developer, which makes them more nimble and adaptive when compared to the Army's lengthy research, development, test, evaluation, and acquisition processes. Adversaries capitalize on cyberspace and electromagnetic capabilities and activities, while those capabilities and activities too often have been peripheral to the Army's normal operations. To seize and maintain the operational and tactical advantage against adaptive adversaries, the Army must make cyberspace central to its operations requiring capabilities and the corresponding subject matter expertise to apply them.

b. In the near-term, the Army science and technology community will focus on developing suitable protection technologies that enhances the resilience and agility of the Army's tactical networks. Providing technologies to help enhance cyberspace situational understanding, defend in depth, and dynamic cyberspace defense requires investments in a broad set of technology categories to include: anomaly based intrusion detection, response and recovery mechanisms, and others.[41]

c. For the mid through far-term, potential improvements in cyberspace technologies could be realized through advances in computing performance, bio-inspired techniques to enable network self-healing, and improved cloud architectures that offer greater potential for security policy enforcement and management. Improvements in trust assessment and validation, and hardware and software assurance capabilities allows the development of trusted network architecture's even if composed of components not fully trusted. The Army will remain vigilant against potential game changing technologies that could jeopardize the security posture of its networks; for example, 3D printing could allow malicious counterfeit components to invade the supply chain and the power of quantum communication techniques could allow adversaries to compromise cryptographic algorithms and keying schemes.

C-2. Cyberspace science and technology investment areas

a. To ensure future capability superiority the following science and technology investment areas for the near term should be addressed:

(1) Cyber situational understanding. Situational understanding in cyberspace is developed through a family of interactive, interoperable, and critical technologies that will facilitate maneuver planning, collaboration, and synchronization through integration with the commander's user-defined operational picture. Technologies that support situational understanding in cyberspace will be fielded within the Army's command post computing environment, establishing a framework to integrate fielded and emerging cyberspace capabilities into combat operations.

(2) Integrated EW. As wired and wireless technology use, has proliferated the Army has become more dependent on these technologies. This dependence places emphasis on developing and operationalizing EW as an integrated battlefield capability that enhances situational understanding, improves force protection, enables dominant maneuver, and aids in precision lethality.

(3) Enhanced SMO. SMO are the interrelated functions of EMS resources managing, frequency assignment, host nation coordination, and spectrum management policy monitoring that enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations.

(4) Future waveforms. To bring cyberspace operations to the tactical edge, the Army will develop and implement upgrades to tactical networking waveforms to increase capacity, flexibility, robustness, and simplicity of operations. The waveform(s) will provide high

throughput (data rates that support tactical requirements) to users within a tactical area of operations and utilize advanced low probability of intercept, detect, and exploit technologies.

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

b. Changes in the cyberspace domain continue to accelerate. In the last two decades, cyberspace has transformed radically how the Army operates and wages war. This transformation is not complete. Cyberspace will continue to grow, and is projected to reach over 100 billion connected devices within the next 10 years. The Army should monitor the following technologies as potential areas of far-term investment.

(1) Autonomous active cyber defense. Develop systems which provide the ability for autonomous network defense through a collection of synchronized, real-time capabilities to discover, define, analyze, and mitigate cyber threats and vulnerabilities without direct human intervention. This capability includes sensor-based artificial intelligence that learns and manages network topologies.

(2) Defensive cyber operation tools. Provide the ability for the network to absorb the shock of a cyber-attack, identify adversary actions, respond with pre-determined actions, and ensure mission continuity. The DODIN-A will assess, compose, and deploy cyber elements with known and predictable confidence in their identity, functionality, and content. The Army leverages a joint and holistic industry approaches to develop secure systems that adapt and maneuver automatically to reduce, counter, and evade cyber-attacks. Capabilities associated with DCO tactical support and enhance cyber situational understanding efforts.

(3) Autonomous cognitive radio frequency. A capability that provides a fully adaptive and reconfigurable radio frequency architecture that is agnostic to waveforms and standards. Radios will have a cognitive capability to operate in any frequency band with any modulation using multiple access specifications, depending on the restrictions of the environment and overall EM operating conditions.

(4) Assured PNT. Assured PNT is a cross cutting capability that provides access and integrity to PNT information in global positioning system-denied environments. Assured PNT focuses on providing resilient and robust PNT, in a scalable architecture, that spans various levels of protection or PNT assurance levels. As technological threats increase, Assured PNT focuses on developing a resilient PNT capability for the Army.

(5) Communications under extreme radio frequency conditions. Provide technologies and techniques that address communications in severe jamming situations and adapt to various jamming and interference sources. The technical objective is to innovate and integrate capabilities through all domains for adaptive interference suppression. This technology development phase

will establish relevant technologies appropriate for the constraints and typical missions of various platforms.

Appendix D
Risk

a. There are some potential risks associated with adopting the ideas proposed in this concept. Therefore, commanders, leaders, and force developers at all levels must devise and implement strategies to manage risk.

b. Inadequate integration of cyberspace operations into operational planning may result in Army units not achieving the full effects of combined arms or benefitting from the cross-domain effects of cyberspace operations. It also places the Army's contribution to joint combined arms operations at risk. Commanders can mitigate this risk through education and training to ensure staff and planners understand the value and application of cyberspace operations, and then reinforce their integration during all command post and field training events.

c. Insufficient resilience in systems may result in an inability to exercise mission command. The Army can mitigate this risk through proper investment and allocation of resources and personnel ensure resilient systems, increase cybersecurity technologies, training, and policies, and by routinely training in degraded environments.

d. Over reliance or dependence on information and communication systems and technologies may result in Army forces becoming incapable of operating in the absence of those systems and technologies. The Army can mitigate this risk by reinforcing basic skills in the event it is faced with operating in a degraded cyberspace environment.

e. The current acquisition process is not able to develop, field, and sustain cyberspace operations capabilities in a timely manner. Failure to acquire emerging technology rapidly and adapt organizations and doctrine for their use simultaneously, will put Army forces at a disadvantage when compared to peer competitors. The Army can mitigate this risk by streamlining the requirements process, improving capability development management, and pushing for reform of the defense acquisition process. The Army must also accept some level of risk to utilize commercial off-the-shelf technologies effectively and seek innovation by Soldiers at the tactical level of operations.

Glossary

Section I
Abbreviations

ACC	Army Capstone Concept
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AFC-MC	Army Functional Concept for Mission Command

AOC	Army Operating Concept
DCO	defensive cyberspace operations
DIV	division
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, education, personnel, facilities, policy
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EW	electronic warfare
FM	field manual
JP	joint publication
SMO	spectrum management operations
TRADOC	United States Army Training and Doctrine Command
TP	TRADOC Pamphlet
TTP	tactics, techniques, and procedures
U.S.	United States

Section II
Terms

assign
To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel. (JP 3-0)

assumption
A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. (JP 5-0)

attach
The placement of units or personnel in an organization where such placement is relatively temporary. (JP 3-0)

civil considerations
The influence of man-made infrastructure, civilian institutions, and activities of the civilian leaders, populations, and organizations within an area of operations on the conduct of military operations. (Army Doctrine Reference Publication (ADRP) 5-0)

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

commander's intent
A clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, 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. (ADRP 6-0)

constraint
A restriction placed on the command by a higher command; dictates an action or inaction, thus restricting the freedom of action of a subordinate commander. (FM 6-0)

cybersecurity
The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (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
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 electronic). (ADRP 6-0)

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 1-02)

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 1-02)

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.

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)

electronic attack
Division of electronic 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 3-13.1)

electronic warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-13.1)

execution
Putting a plan into action by applying combat power to accomplish the mission. (Army Doctrine Publication (ADP) 5-0)

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)

inform and influence activities
The integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decision-making. (ADRP 3-0)

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

information-related capabilities
Capabilities, techniques, or activities employing information to effect any of the three dimensions within the information environment to generate an end(s). (FM 3-13)

information warfare
Information warfare spans several capabilities and functions such as: military information support operations; military deception; operations security; EW; physical attack; special technical operations; information assurance; DODIN-A operations; public affairs; and civil- military operations.

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

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
Any information element the commander and staff require to successfully conduct operations. (ADRP 6-0)

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. (FM 6-0)

joint combined arms operations
Synchronized, simultaneous, or sequential application of two or more arms for elements of one service, along with joint, interorganizational, and multinational capabilities combined with leadership and education across services to ensure unity of effort and create multiple dilemmas for the enemy to seize, retain, and exploit the initiative. (AOC)

joint electromagnetic spectrum operations
Those activities consisting of electronic 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)

joint operational planning process
An orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best course of action, and produce a joint operation plan or order. (JP 5-0)

measure of effectiveness
A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 3-0)

measure of performance
A criterion used to assess friendly actions that is tied to measuring task accomplishment. (JP 3-0)

military decision-making process
An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

mission command
The exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of joint combined arms operations. (ADP 6-0)

mission command warfighting function
The related tasks and systems that develop and integrate those activities enabling a commander to balance the art of command and the science of control in order to integrate the other warfighting functions. (ADRP 3-0)

mission orders
Directives that emphasize to subordinates the results to be attained, not how they are to achieve them. (ADP 6-0)

mission statement
A short sentence or paragraph that describes the organization's essential task(s), purpose, and action containing the elements of who, what, when, where, and why. (JP 5-0)

monitoring
Continuous observation of those conditions relevant to the current operation. (ADRP 5-0)

multi-domain battle
Cross-domain operations that create temporary windows of superiority across multiple domains, and allow Joint Forces to seize, retain, and exploit the initiative.

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

operation order
A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. (JP 5-0)

operational control
The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. (JP 1)

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. (ADRP 5-0)

priority intelligence requirement
An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or other aspects of the operational environment. (JP 2-01)

risk management
The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. (JP 3-0)

running estimate
The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

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)

Section III
Special terms

cyber electromagnetic activities
The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations. (Proposed)

electromagnetic spectrum
(For the purposes of this pamphlet the EMS is defined as), the range of frequencies of electromagnetic radiation that has been allocated for specified services under the U.S. and international tables of frequency allocation.

electromagnetic spectrum operations
Those activities consisting of electronic warfare and spectrum management operations used to exploit, attack, protect, and manage the electromagnetic operational environment to achieve the commander’s objectives. (Proposed EMSO definition based on Joint Concept for Electromagnetic Spectrum Operations, 15 March 2015, JP 6-01, and FM 3-12)

electromagnetic spectrum superiority
That degree of advantage in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting an adversary’s ability to do the same. (Proposed JCEMSO definition)

End Notes

[1] FM 3-12.
[2] Multi-domain battle is defined as ready ground combat forces capable of outmaneuvering adversaries physically and cognitively through extension of combined arms across all domains. Through credible forward presence and resilient battle formations, future ground forces integrate and synchronize joint, interorganizational and multinational capabilities to create temporary windows of superiority across multiple domains; seize, retain, and exploit the initiative; and achieve military objectives. Army-Marine Corps Multi Domain Battle White Paper.
[3] Cyber mission forces includes the Cyber National Mission Force (CNMF), the Cyber Combat Mission Force (CCMF), Cyber Protection Force (CPF), Cyber National Mission Force Headquarters (CNMF-HQ), Joint Force Headquarters- Cyber (JFHQ-C), the JFHQ-DODIN, and the Enterprise Operations Centers (EOCs). (Joint Cyberspace Concept)
[4] This ROE will address the challenges associated with domestic challenges to CIKR and DSCA. While operational preparation of the environment consists of non-intelligence enabling activities to plan and prepare for potential follow-on military operations, Intelligence will be conducted to support the commanders planning and preparation. Intelligence support to CO utilizes the same intelligence process as in all other military operations.
[5] A single, joint, secure, reliable, and agile command, control, communications and computing enterprise information environment.
[6] Joint Cyberspace Concept. The DOD will also recognize the challenges associated with joint information environment implementation.
[7] Joint Operating Environment 2035.
[8] The OE describes the composite conditions, circumstances, and influences that affect commanders' decisions on the employment of military capabilities. [JP 3-0] [TP 71-20-3 The U.S. Army Training and Doctrine Command Concept Development Guide]
[9] ACC.
[10] Capstone Concept for Joint Operations: Joint Force 2020.
[11] Joint Operating Environment 2035
[12] U.S. Army TRADOC Pamphlet 525-3-0, The U.S. Army Capstone Concept.
[13] Department of Homeland Security – Industrial Control Systems Cyber Emergency Response Team, Cyber Threat Source Descriptions https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.
[14] TRADOC PAM 525-8-3, The U.S. Army Human Dimension Concept, 21 May 2014.
[15] Joint Cyberspace Concept.
[16] Joint Cyberspace Concept.
[17] AOC.
[18] AOC.
[19] AOC.
[20] AOC.
[21] ACC
[22] Joint Cyberspace Concept.
[23] Joint Cyberspace Concept.
[24] Joint Cyberspace Concept.
[25] Joint Cyberspace Concept.
[26] Joint Cyberspace Concept.
[27] Dual-use technologies are those that share military and civilian application. Typically used to describe civilian technologies employed by the military, they may also include military technological advancements that find their way into civil use. Examples include GPS, radar, and night vision goggles.
[28] A cognitive radio is an intelligent, dynamically reprogrammable, and reconfigurable device that automatically detects the optimal transmission or reception parameters based on available bandwidth in the local EMS.
[29] Cyberspace operations missions include (1) DODIN operations, (2) DCO, and (3) offensive cyberspace operations. (FM 3-12(R))
[30] ACC.
[31] ACC.
[32] TRADOC PAM 525-8-3.
[33] ACC.
[34] Innovation is the act or process of introducing something new, or creating new uses for existing designs.
[35] AOC.
[36] AOC.
[37] ACC.
[38] TRADOC PAM 525-8-3.
[39] Field Manual 3-12.
[40] Joint Concept for Electromagnetic Spectrum Operations.
[41] Others include: continuous risk monitoring and sensing, mapping of cyberspace-attacks to mission impact, data-at-rest security support, biometric techniques to improve blue force access control, a unified public key infrastructure certificate validation architecture, forensics techniques, automated source code analysis tools, non-destructive hardware assurance tools, and system and network obfuscation techniques to support cyberspace maneuver.