

---

**THE U.S. ARMY  
LANDCYBER WHITE PAPER  
2018-2030**

---

**9 September 2013**

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

**U.S. Army Cyber Command/2<sup>nd</sup> U.S. ARMY  
Army Cyber Proponent  
Fort George G. Meade, MD 20755**

## Report Documentation Page

*Form Approved*  
*OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>09 SEP 2013</b>	2. REPORT TYPE <b>N/A</b>	3. DATES COVERED <b>-</b>	
4. TITLE AND SUBTITLE <b>U.S. Army LandCyber White Paper 2018-2030</b>		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>U.S. Army Cyber Command/2nd U.S. ARMY Army Cyber Proponent Fort George G. Meade, MD 20755</b>		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) <b>U.S. Army Capabilites Integration Center</b>		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release, distribution unlimited</b>			
13. SUPPLEMENTARY NOTES <b>The original document contains color images.</b>			
14. ABSTRACT <b>a. This white paper describes Army cyberspace operations in the 2018-2030 timeframe consistent with evolving joint cyber doctrine and directives. It identifies Army cyberspace equities in the joint fight; identifies needs and requirements across the Armys warfighting functions (WfFs); identifies and clarifies capabilities influencing joint interoperability; informs planning, programming, budgeting, and execution process; and as appropriate, prioritizes capabilities, assesses status, identifies key requirements; and recommends key decision points and milestones requiring Army action. It specifically informs the Total Army Analysis and Program Objective Memorandum processes, CBA and CNA processes, and the DOD Executive Agent for cyberspace.</b>			
15. SUBJECT TERMS			
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>	<b>SAR</b>
			18. NUMBER OF PAGES <b>54</b>
			19a. NAME OF RESPONSIBLE PERSON

Intentionally blank

## Foreword

### **From Commanding General U.S. Army Cyber Command/2<sup>nd</sup> Army**

Historically, armies defined themselves geographically; a line on a map measured success. Cyberspace transcends geography and conventional borders, real and imagined. Cyberspace provides America's competitors and enemies an asymmetric, multi-dimensional aim point to strike at the core of a previously uncontested advantage in time and space across the range of military operations. Cyberspace pervasively extends to and throughout all echelons of Army down to the individual Soldier. Cyberspace is pervasive; it presents a problem that demands the Army re-conceptualize time and space to win future battles and wars.

Cyberspace threats are real, sophisticated, growing, and evolving. The Army must recognize that adversaries want to undermine its ability to operate freely and then train, organize, and equip to take full advantage of cyberspace potential. The Army must anticipate disruption attempts, plan for an adversary's potential ability to destroy friendly networks, and account for the impacts of social networks on Army operations.

The advent of a globally interconnected populace via the Internet created a technological and social revolution that extended human lives and social discourse from the physical environment into the virtual environment of cyberspace. The Army has witnessed consequential shifts in human affairs as cyberspace has enabled considerable influence over human and machine behavior. Failure to adapt to this new operational duality (the convergence of the land and cyberspace domains to allow integrated LandCyber operations) cedes the initiative in cyberspace to future adversaries, narrows the Army's understanding of the human context, and unnecessarily limits our maneuver and influence options in a complex, continuously evolving, rapidly expanding strategic environment. The Army must think globally and act locally within the joint operations construct in the cyberspace domain in concert with land forces and humans to shape the physical and virtual behavior of human populations and machines to its opportunity and advantage. The convergence of time and space, technology and functional synergy increasingly drives the Army to find ways to seamlessly integrate and unify the operational and institutional force.

Cyberspace operations are critical to the Nation and the Army's mission, and the Army recognizes the need to organize and operate in this new domain as part of the joint force. Cyberspace operations involve multiple disciplines each using inherent capabilities. There are challenges and opportunities in cyberspace that warrant new kinds of joint operational and institutional integration to form warfighting platforms and functions in cyberspace that achieve advantage and deter adversaries.

To defend and advance national interests, the Army must balance resources and risk to prepare and conduct the Army's three roles of prevent, shape, and win with unified action partners. Prevent conflict by maintaining credibility based on capacity, readiness and modernization; shape the environment by sustaining strong relationships with other armies,

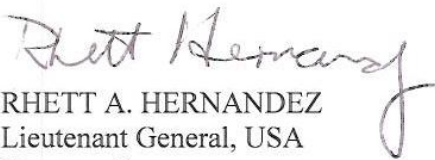
building their capacity, and facilitating strategic access; and, win decisively by applying combined arms capabilities to dominate the operational environment.

The Army must become one that is organized, trained, and equipped to shape human and machine behavior on land and in cyberspace. LandCyber is a transformational concept that deals with cross-domain dynamics and accounts for what is fundamentally new about the operational environment, which is the emergence of a new domain that has moved activity relevant to land operations outside traditional areas of operations. At the same time, cyberspace has made the physically constrained U.S. Army vulnerable to the range and influence of cyber-organized, trained, and equipped adversaries.

The operation and employment of land and cyber forces under a LandCyber framework requires the integration of multiple disciplines in new and innovative ways providing the capabilities required to support land force commanders. LandCyber will define these constructs and will account for what is fundamentally different about this new domain and operational environment.

LandCyber is a unified overarching operational and institutional solution framework to account for cyberspace to all aspects of Army operations. It transforms an Army dominant on the ground into an Army able to sustain operations in and among populations active physically on land and virtually in cyberspace. Under the integrating construct of mission command, LandCyber enables commanders to visualize operationally relevant activities across land and cyberspace domains; conduct simultaneous, linked maneuver over land and cyberspace; engage populations wherever they live and operate; and tailor the full range of physical and virtual force into combinations that ultimately address the underlying motivations for group behavior. Adopting this approach provides future Army forces with unprecedented understanding, range, speed, operational and organizational agility, influence, and the capability to engage target populations from anywhere on Earth.

LandCyber endstate is an Army that is part of a joint team, operationally engaged, active in prevention and in shaping the operational environment regardless of its location and whose forces are disproportionately more powerful, agile, elusive, adaptive, and capable. With LandCyber, mission command, intelligence, movement and maneuver, fires, sustainment, protection, and human and social interaction will come together to ensure the Army is “second to none” in cyberspace.

  
RHETT A. HERNANDEZ  
Lieutenant General, USA  
Commanding

## **Executive Summary**

### **1. Framing the problem**

a. The convergence of land and cyberspace operations is driving transformational change in Army operations. Land and cyberspace operations will continue to converge creating increased interdependence and, coupled with the momentum of human interaction, create complex operating environments.

b. The Army depends on cyberspace to function and create the necessary effects to gain an information advantage over adversaries. Commanders and leaders at all echelons and locations use cyberspace to conduct the range of military operations enabling military, intelligence, and business operations. The services' reliance on cyberspace is the basis for the July 2011 DOD Strategy for Operating in Cyberspace.

c. The majority of land operations will occur among populations. Adversaries will attempt to control the narrative and deny the use of information and communications technologies (ICT) to their own populations, especially in areas where information, unified action partner partnerships, and legitimacy are key enablers to the United States (U.S.) cyberspace strategy. Cyberspace has made the physically constrained Army vulnerable to the range and influence of cyber-organized, trained, and equipped adversaries.

d. As technology evolves, threats from state and non-state actors will continue to evolve and proliferate. The widespread availability of ICT capabilities allows less technologically advanced adversaries to seek strategic to tactical advantage over U.S. capabilities without investment in technological development. Army formations will require access to dynamic cyber capabilities to retain an advantage over adversaries leveraging proliferated cyber tools.

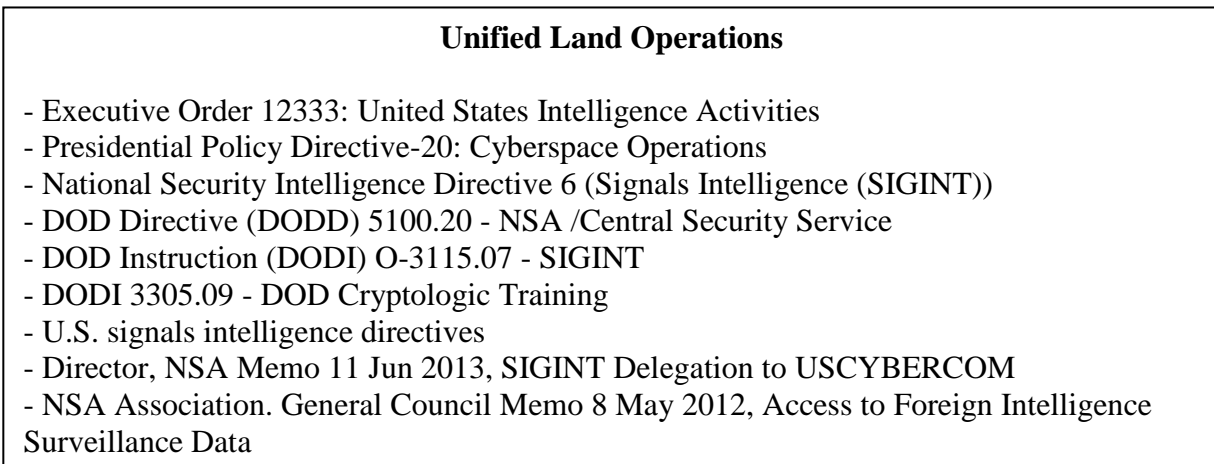
e. Army forces will be U.S. based, deploying into areas where access is contested and network and electromagnetic links across organizations, systems, functions and tasks will be challenged. The use of fiber optic, electromagnetic, and laser technologies to pass digital data, information, plans, orders, and commands to weapons systems will challenge the best technical means available to the U.S. including close access capabilities to bridge the global Internet, electromagnetic, space and air gaps.

### **2. Framing the solution**

a. The U.S. Army LandCyber White Paper 2018-2030 describes a transformational concept that deals with emerging cross-domain dynamics, land and cyberspace, while accounting for fundamental changes in the operational environment. The emergence of relevant and significant human activity to directly or indirectly – in or through the cyberspace domain – effect change in other domains and human populations more traditionally defined by geography, sovereignty, and/or graphic control measures.

b. The ideas described in this paper acknowledge that commanders operating in cyberspace are governed by laws, policies, regulations, and rules of engagement that must be understood and

integrated into planning, coordinating, and executing cyberspace operations. The capabilities required to execute all offensive and some defensive cyberspace operations are enabled by intelligence operations on the National Security Agency's (NSA) cryptologic enterprise, and as such, subject to significant regulations and oversight, (see figure 1). Commanders at all levels must be educated on these restrictions as failure to enforce governing intelligence policies, classification, and oversight requirements could result in compromise or unauthorized activity.



**Figure 1. Cyberspace related polices and directives**

c. The ideas described in this paper acknowledge that the Army Chief Information Operating Officer (CIO)/G-6 exercises responsibilities on behalf of the Secretary of the Army for network operations oversight and execution, network architecture development and implementation, information security governance and enforcement, information technology (IT) budget and acquisition oversight and execution, and IT workforce oversight and enforcement, as defined in US Code Title 10, Section 2223; Title 40, Section 11315; Title 40, Chapter 35 and Section 3534; and the 2002 Federal Information Security Act. The CIO/G-6 's efforts are focused on LandWarNet 2020 and beyond modernization initiatives (see figure 2) that will transform the Army's network into a unified defensible enterprise consistent with the Joint Information Environment enabling cyberspace operations and the viability of the Army network into the future.

## **Army CIO/G-6 LandWarNet Modernization Initiatives**

Network capacity:

- Wide area network – Increase capacity and speed
- Transport convergence – Converge voice, video, and data on a single network infrastructure; everything over Internet protocol

Enterprise services:

- Voice over Internet protocol – enhanced collaborative capabilities that span all devices
- Unified capabilities – multiple forms of communication and collaboration through a single device

Network operations and security:

- Re-engineer top-level architecture – simplify and standardize network, increase performance and enforce compliance
- Identity management – improve access control to systems and data via a single sign-on capability

**Figure 2. LandWarNet 2020 modernization initiatives**

### **3. Solution context: Land-cyber-human**

a. LandCyber operations offer a transformational outcome similar to the Army's AirLand Battle effort of the 1980s that, when fully instantiated, will ensure optimal integration of land and cyber effects to influence the threat before it impacts friendly forces and operations. Under the integrating construct of mission command, LandCyber operations generate and exert combat power in and through cyberspace to enable freedom of maneuver and action in both the land and cyberspace domains and deliver decisive effects.

b. LandCyber operations enable commanders to visualize operationally relevant activity across both domains, conduct simultaneous, linked operations in land and cyberspace, engage populations wherever they live and operate, and tailor the full range of physical and virtual forces into combinations that ultimately address the underlying motivations for group behavior. Adopting this approach provides future formations with unprecedented range, speed, agility, influence, social, and cultural perspective with the capability to engage target populations from anywhere on Earth.

### **4. Central idea**

The Army must think globally and act locally in the cyberspace domain, in concert with land forces and the human aspects of conflict and war, to shape the security-related behavior of humans and their machines to its opportunity and advantage. This requires evolution of a seamless operational and institutional framework that purposely enables the generation and application of cyber combat power to support commanders on land and in cyberspace.

### **5. Solution framework**

a. The Army has attempted, through previous concepts such as TRADOC PAM 525-7-8, to address the broad range of tasks associated with cyberspace that have evolved over time from a set of tasks to a domain with consequences for land forces and human populations that must be



captured in the commander’s concept of the operation. The LandCyber framework outlined in this white paper attempts to address how cyberspace links to the land commander’s area of responsibility, area of interest, and area of influence by describing how it nests with the joint cyberspace operations construct evolving under USCYBERCOM to describe Army operating concepts in this domain.

b. The solution accounts for eight aspects of convergence with significant implications for the Army and provides an operational and institutional framework based on nine guiding principles listed in table 1 below:

**Table 1**  
**Aspects of convergence and guiding principles to solution framework**

Eight Aspects of Convergence	Nine Guiding Principles
1. Time and space	1. Unified cyberspace operations
2. Threat and technology	2. Integration
3. Land and cyber domains	3. Localized cyberspace effects to the tactical edge
4. Cyberspace and electromagnetic spectrum	4. Enhanced understanding
5. Defensive and offensive cyber operations	5. All networks are operational warfighting platforms and functions
6. Information environment and cyberspace domain	6. Combined arms approach
7. Information management and knowledge management	7. Achieve cyberspace domain superiority
8. Operational and institutional	8. Ensure mission command
	9. Empowered LandCyber units and Soldiers

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

9 September 2013

**Military Operations**

**U.S. ARMY LANDCYBER WHITE PAPER 2018-2030**

---

**History.** This white paper is a new publication that renders the Training and Doctrine Command (TRADOC) Pamphlet (Pam) 525-7-8, dated 22 February 2010 obsolete. The white paper is nested fully with the central and supporting ideas of Army 2020, TRADOC Pam 525-3-0, and TRADOC Pam 525-3-1.

**Summary.** This white paper describes Army cyberspace operations in the 2018-2030 timeframe, to include Army cyberspace operations needs and required capabilities. It informs Total Army Analysis process, capabilities based assessments (CBA), and formation based capabilities needs assessments (CNA). As such, the Director, Army Capabilities Integration Center (ARCIC) endorses the white paper.

**Applicability.** This white paper applies to all Department of Army (DA), U.S. Army Reserve and U.S. Army National Guard component activities that develop Army cyberspace doctrine, organization, training, materiel, leadership and education, personnel, and facilities requirements and capabilities. It applies to future Army cyberspace force development, CBAs, and Joint Capabilities Integration and Development System documents, experimentation, and doctrine pertaining to Army cyberspace operations. It serves as a source of information to update the concepts within the Army concept framework. It supports science and technology challenges and experimentation described in the ARCIC Concepts and Capabilities Guidance as the conceptual basis for developing solutions to the future force for Army cyberspace operations.

**Proponent and supplementation authority.** The proponent of this paper is the TRADOC Headquarters, Director, ARCIC. The proponent has the authority to approve exceptions or waivers to this paper that are consistent with controlling law and regulations. Do not supplement this paper without prior approval from Director, TRADOC ARCIC (ATFC-ED), 950 Jefferson Avenue, Fort Eustis, VA 23604-5763.

**Suggested improvements.** Users are invited to 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 to Director, TRADOC ARCIC (ATFC-ED), 950 Jefferson Avenue, Fort Eustis, VA 23604. Suggested improvements may also be submitted using DA Form 1045.

**Availability.** This pamphlet is available on the ARCIC Portal at <https://cac.arcicportal.army.mil/sites/cde/condev/White%20Papers%20and%20CONOPS/Forms/AllItems.aspx>

<b>Contents</b>	<b>Page</b>
Foreword	iii
Executive Summary	v
<b>Chapter 1. Introduction</b>	<b>3</b>
1-1. Purpose	3
1-2. Background	3
1-3. References	4
1-4. Explanations of abbreviations and terms	5
<b>Chapter 2. Operational Context</b>	<b>5</b>
2-1. The strategic environment	5
2-2. Cyberspace as a domain	6
2-3. Cyberspace and the operational environment	7
2-4. Emerging cyberspace operations	7
2-5. Defensive cyberspace operations	7
2-6. Offensive cyberspace operations	8
2-7. LandCyber in the Army's prevent, shape, and win roles	8
<b>Chapter 3. Military Problem and Components of the Solution</b>	<b>9</b>
3-1. Military problem	9
3-2. Central idea	9
3-3. Solution synopsis	9
3-4. Components of the solution and supporting ideas	12
<b>Chapter 4. Army WfFs, Human Aspect of Conflict, and Cyberspace Capabilities</b>	<b>17</b>
4-1. Introduction	17
4-2. Cyberspace capabilities across warfighting functions	17
4-3. The human aspect of conflict in cyberspace	22
4-4. Summary	22
<b>Chapter 5. Conclusion</b>	<b>23</b>
<b>Appendix A. References</b>	<b>24</b>
<b>Appendix B. Required Capabilities</b>	<b>29</b>
<b>Appendix C. Facts and Assumptions</b>	<b>32</b>
<b>Appendix D. Implications and Risks</b>	<b>34</b>
<b>Appendix E. Future Army Institutional Force Framework</b>	<b>35</b>
<b>Glossary</b>	<b>38</b>

## **Chapter 1 Introduction**

### **1-1. Purpose**

a. This white paper describes Army cyberspace operations in the 2018-2030 timeframe consistent with evolving joint cyber doctrine and directives. It identifies Army cyberspace equities in the joint fight; identifies needs and requirements across the Army's warfighting functions (WfFs); identifies and clarifies capabilities influencing joint interoperability; informs planning, programming, budgeting, and execution process; and as appropriate, prioritizes capabilities, assesses status, identifies key requirements; and recommends key decision points and milestones requiring Army action. It specifically informs the Total Army Analysis and Program Objective Memorandum processes, CBA and CNA processes, and the DOD Executive Agent for cyberspace.

b. The required Army cyberspace capabilities and conclusions in this paper are based upon comprehensive analysis of the key concepts that comprise the Army 2020 the Army Concept Framework, the evolving joint cyberspace operations framework, and the legal, policy, inter-agency environment inherent to conducting operations in the cyberspace domain.. The ideas expressed provide the overarching conceptual framework for Army cyberspace operations integrated across the range of military operations. It renders TRADOC Pam 525-7-8, obsolete.

### **1-2. Background**

a. Cyberspace in support of unified land operations (ULO).

(1) As America's principal land force, the Army conducts responsive and sustained combat operations in order to fight as part of a joint team and to respond, as directed, to crises at home and abroad. Army doctrine describes this as ULO.<sup>1</sup> In 2011, the DOD Strategy for Operating in Cyberspace provided guidance to treat cyberspace as an operational domain; to seize the initiative and take full advantage of cyberspace potential.

(2) In 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish USCYBERCOM. The USCYBERCOM mission is to plan, coordinate, integrate, synchronize and conduct activities to direct the operations and defense of specified DOD information networks; prepare to, and when directed, conduct full spectrum military cyberspace operations to enable actions in all domains; ensure U.S. and allied freedom of action in cyberspace and deny the same to adversaries.

(3) The Army established the Army Cyber Command (ARCYBER)/2nd Army in 2010.<sup>2</sup> Its mission is to plan, coordinate, integrate, synchronize, direct, conduct network operations, and defend all Army networks; when directed, conduct cyberspace operations in support of the range of military operations to ensure U.S. and allied freedom of action in cyberspace, and to deny the same to adversaries.

---

<sup>1</sup> ADP 3-0, p. 5-6.

<sup>2</sup> General Order 2010-26, 01 Oct 2010.

(4) Execute order (EXORD) 155-10 established the Army cyberspace proponent and directed proponent actions to coordinate cyberspace operations with TRADOC, Army commands, Army service component commands, (ASCCs), direct reporting units, forward operating agencies, Headquarters DA staff, and other organizations and commands. The Army cyber proponent, provides recommendations through TRADOC to the Chief of Staff of the Army for decision regarding cyber proponentcy.

b. The Army's role and responsibilities in cyberspace as an institution.

(1) Roles and responsibilities include provisioning a service component to USCYBERCOM and provisioning organized, trained, and equipped forces ready for combat operations to include operations in the cyberspace domain. Institutional responsibilities call for provisioning cyber leader and force development, education and training, and developing as well as providing concepts for unified LandCyber operations, nested in the Joint Cyberspace Operations and Training construct. Institutional force considerations are in Appendix E.

c. The Army's roles and responsibilities in cyberspace as an operating force.

(1) Support prevent, shape, and win roles with cyberspace capabilities. This requires supporting intelligence operations and conducting cyberspace operational preparation of the environment (OPE) to plan and prepare for military operations. Building, operating and defending all Army networks as an end-to-end enterprise ensures its availability to the Army.

(2) Provide critical infrastructure protection for the Army and U.S. Northern Command national systems, and provide Army-wide indications and warning against threats and attacks.

(3) Integrate cyberspace operations capabilities into joint and Army planning and exercises, facilitate security cooperation to create defense in depth (under the direction of COCOMs and subject to the limitations of National Foreign Disclosure Policy), develop shared indications and warning, and leverage combined cyberspace operations strengths. Plan and integrate world-class cyber opposing forces (WCCO) in concert with USCYBERCOM and provide representative adversary command, control, and networked systems into training, testing, experiments, and exercises. This integration develops Army forces that can detect and respond to adversary cyber attacks and operate in a degraded cyberspace environment.

(4) Integrate cyberspace operations into combatant command planning and targeting processes to broaden the range of options. Deliver offensive and defensive cyber effects, if approved and directed, planned and integrated through cyber electromagnetic activities (CEMA). Conduct information operations (IO) in or through the cyberspace domain for the Army and support inform and influence activities (IIA) in or through the cyberspace domain. Other considerations are in chapter 3.

### **1-3. References**

Required and related publications are listed in appendix A.

## **1-4. Explanation of abbreviations and terms**

Abbreviations and special terms used in this white paper are explained in the glossary.

---

## **Chapter 2 Operational Context**

### **2-1. The strategic environment**

#### **a. Background.**

(1) Strategic organizational environment. In 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish USCYBERCOM.<sup>3</sup> The USCYBERCOM mission is to plan, coordinate, integrate, synchronize and conduct activities to direct the operations and defense of specified DOD information networks; prepare to, and when directed, conduct full spectrum military cyberspace operations to enable actions in all domains; ensure U.S. and allied freedom of action in cyberspace and deny the same to adversaries. The Secretary of Defense also directed the services to provide component support to USCYBERCOM. Subsequently, ARCYBER was established and assigned to U.S. Strategic Command in the global force management process, with operational control of the command delegated to USCYBERCOM.

(2) Strategic policy environment. There are long standing operations and intelligence policy constraints regarding the role of the DOD and the intelligence community in cyberspace operations that will continue to shape the evolution of Army cyberspace operations. National policy reinforces the level of oversight and control required for cyberspace operations and retains intelligence operations in cyberspace as separate and distinct functions. Commanders at all levels must be educated on the governing intelligence policies, classification and oversight requirements, as failure to do so could result in compromise or unauthorized activity.

#### **b. Near-term.**

(1) The cyberspace domain will continue to grow more contested, congested, and competitive and represent one of the most direct approaches for strategic, operational, and tactical attack by adversaries using a variety of threat vectors. The majority of land operations will occur among populations. Adversaries will attempt to control the narrative and deny the use of information and communications technology (ICT) to their populations, especially in areas where information, unified action partners, and legitimacy are key enablers to the U.S. strategy. State sponsored threats will leverage existing technologies through commercial off-the-shelf acquisitions and technological transfers in pursuit of dominance over U.S elements of national power. The growing presence of ICT in operational environments (OE) will create a wide range of opportunities and vulnerabilities across CEMA capabilities, tactics, techniques, and procedures.

---

<sup>3</sup> SECDEF Memo, Establishment of a subordinate Unified Cyber Command under U.S. Strategic Command, 23 Jun 2009.

(2) The physical infrastructure and the virtual aspect of the cyberspace domain will create a rapidly evolving OE with a cyberspace infrastructure that is dynamically established, changed, moved, and disestablished to suit the needs and desires of friendly, neutral, and enemy participants in the area of responsibility (AOR). The Army will continue to strive for an enterprise information environment comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies in accordance with the joint information environment (JIE) concept.

b. Mid-term. Army networks will be built and operated as warfighting platforms that perform functions focused on delivering tailored effects. Land and cyberspace operations will continue to converge creating increased interdependence. As technology evolves, the threat from state and non-state actors will continue to evolve and proliferate. Commoditization of ICT capabilities will enable a wide array of threat actors not traditionally associated with advanced technology and advanced effects to seek strategic-to-tactical advantage over U.S. capabilities. The unified land commander will require access to dynamic cyber capabilities to retain an advantage over adversaries leveraging proliferated cyber tools. The transformation to the JIE will enhance connectivity, access, defense, and governance of the LandWarNet.<sup>4</sup> However, the utilization of largely commercial off-the-shelf cloud-based technology will enable threats seeking similar advantages. Threats will leverage cyber capabilities to nullify an otherwise U.S. technological overmatch.

c. Long-term. In the future, adversaries will plan and rehearse the execution of their operations utilizing simulation or gaming technology aided by artificial intelligence that replicates real terrain, physical structures, and social interaction in cyberspace. The effects will be delivered physically and in cyberspace. Participants in the fight may never meet face-to-face during the plan, prepare, execute, and assess process. Army forces will be U.S.-based predominantly, deploying into areas of contested access with links to critical enablers severely challenged. The use of fiber optic, electromagnetic, and laser technologies to pass digital data, information, plans, orders, and commands to weapons systems will challenge the best U.S. technical means, requiring emphasis on close access capabilities to bridge the global Internet, electromagnetic, space, and air gaps.

## **2-2. Cyberspace as a domain**

There are strategic consequences associated with the domains. For a nation to have access to the world and its resources, it must be a land, air, sea, space, and cyber power. To project land forces and lethal effects around the globe to secure national interests, a nation must be an air and maritime power. To practice effective mission command, sustain the forces, provide critical intelligence, and communicate over the horizon, a nation must be a cyber and space power. To withstand or encourage the weight and momentum of human interaction to alter the OE to advantage, a nation must also be a cyber power. Cyberspace represents the most operational form of the information environment (IE). Cyberspace is terrain that sustains collective activity and shapes the security related behavior of humans and their machines.

---

<sup>4</sup> LandWarNet is the Army's contribution to the global information grid.

### **2-3. Cyberspace and the OE**

a. The Army has successively developed different frameworks for visualizing the commander's area of operations (AO) in terms of places, people, and things. The physical dimension provides a lens for land, air, maritime, and space domains, and the physical layer of the cyberspace domain, to define boundaries from which to coordinate, deconflict, operate, and secure access. The IE encapsulates the cognitive dimension through which information technology provides the means for individuals, groups, and nation states to influence the outcomes of military operations.

b. A virtual dimension has emerged that requires reconciliation with the physical and cognitive dimensions for commanders to define and operate in their respective OEs. The virtual dimension allows combatants to traverse the physical and cognitive dimensions in time and space, to yield direct and indirect approaches to obtaining a military advantage. The combination of these three dimensions provides the lens through which the OE is understood and the security related behavior of both humans and their machines is influenced. Consequently, the Army must organize, train, and equip for operations in and among human groups on land where they operate physically, cognitively, and virtually.

### **2-4. Emerging cyberspace operations**

a. An emergent operational imperative is a requirement for cyber forces to maneuver in cyberspace to protect and defend the network from attackers, and prepare to use (within appropriate authorities, policies, and rules of engagement) the full range of cyberspace to support of ULO. This requirement ensures U.S. and allied freedom of action in cyberspace, while denying the same to adversaries. Maneuver is the employment of forces in the AO through movement in combination with fires to achieve a position of advantage in respect to the enemy. Consistent with joint cyber constructs and governing principles, cyberspace terrain will be accessed through physical and virtual means along unique avenues of approach to provide the advantage of position for generating effects in the land domain. Joint fires will create specific lethal or nonlethal effects on a target. Joint offensive cyberspace operations will employ nonlethal capabilities as a means to cause malfunction or destruction of enemy equipment that can also lead to personnel injury or loss of life to the adversary.

b. The movement and maneuver WfF comprises the related tasks and systems that move and employ forces to achieve a position of relative advantage over the enemy. Combined arms maneuver is the application of the elements of combat power to achieve physical, temporal, and psychological advantage over the enemy to seize and exploit the initiative. These definitions will extend to include synchronization and maneuver of cyber forces over cyber terrain to achieve a position of advantage in a manner consistent with joint offensive and defensive cyberspace constructs that have evolved under USCYBERCOM.

### **2-5. Defensive cyberspace operations**

a. The unified land commander will identify key terrain on Army networks where critical applications reside and critical information is required to support ongoing military operations.



Army cyberspace defense forces employ passive and active sensors on Army networks to conduct reconnaissance and surveillance on physical and virtual avenues of approach to key terrain. Employed sensors will include network and host-based intrusion detection and prevention capabilities, and anomaly-based detection capabilities integrated with supporting intelligence community capabilities. Counter-reconnaissance, or hunt forces, will work within Army networks to maneuver, secure, and defend key cyberspace terrain, identifying and defeating concealed cyber adversaries that have bypassed the primary avenues of approach monitored by automated systems.

b. Counterintelligence, counter-reconnaissance, and cyber hunt teams will work inside the Army enterprise to actively search for and locate threats that have penetrated the Army enterprise, but not yet manifested their intended effects. Cyber hunt teams, with advanced technical skills, will provide an enhanced defensive posture to protect portions of Army networks for specified missions for the duration of mission execution.

## **2-6. Offensive cyberspace operations**

a. Exploiting or attacking a target in or through cyberspace is a highly complex and regulated joint operation conducted on the U.S. cryptologic enterprise requiring special authorities and accesses to the OE. Intelligence forces identify multiple avenues of approach consistent with joint constructs now defined by USCYBERCOM and the NSAgency. Army intelligence and cyber forces will work with joint partners to identify a target before conducting joint cyber fires to deliver an effect.

b. The schematics for maneuver in cyber are highly complex and dynamic defined by ever changing avenues of approach that include routers, switches, bridges, and servers that provide data transfer, routing, and storage instructions for the data packets. The Army must overcome firewalls, sensors, and other security measure obstacles to gain access and to engineer and deliver a payload to create an effect.

## **2-7. LandCyber in the Army's prevent, shape, and win roles**

a. Globally engaged and regionally responsive, the Army will conduct unified LandCyber operations to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution.

(1) Prevent. Deter adversaries by holding them at risk with credible LandCyber formations and capabilities, which will serve to influence and deter, and enable access for ready and capable LandCyber forces to protect the U.S. and its interest.

(2) Shape. Extend reach and access by LandCyber forces through cyberspace to enable security and stability for all U.S. interests.

(3) Win. Quickly isolate, overwhelm, and dominate the threat on land and cyberspace through unified LandCyber maneuver and action to meet objectives.

b. The LandCyber endstate is an Army as part of a joint team that is operationally engaged, active in prevention and in shaping the OE regardless of its location; with formations disproportionately more powerful, agile, elusive, adaptive, and capable than any adversary.

c. Prevent. Unified land forces, supported by regionally-aligned cyber forces, project a virtual presence into the AOR through joint regional cyber centers with required connectivity and services, to avert adversaries' miscalculations, and capitalize on the ability to gain and maintain access to AOR centers of gravity, populations, and groups.

d. Shape. Incorporating cyberspace OPE, intelligence indications and warnings and a shared situational awareness (SA) of cyberspace threats into operational planning will improve the commander's understanding of the physical, informational, and cognitive dimensions of the IE in which they may conduct operations.

e. Win. When deployed into theater, unified land forces produce a combination of effects in the land and cyberspace domains to achieve their objectives. The unified land commander is enabled with the full range of cyberspace and IIA capabilities.

---

## **Chapter 3**

### **Military Problem and Components of the Solution**

#### **3-1. Military problem**

How does the Army employ cyber capabilities with other elements of combat power in and through cyberspace to support ULO?

#### **3-2. Central idea**

The Army must think globally and act locally in the cyberspace domain in conjunction with land forces to shape the physical and virtual security-related behavior of humans and their machines to gain opportunity and advantage. This requires a new solution framework that purposely enables the generation and application of cyber combat power to support commanders on land and in cyberspace seamlessly.

#### **3-3. Solution synopsis**

a. LandCyber framework. LandCyber is a framework offering a transformational outcome similar to the Army's AirLand battle effort of the 1980s.<sup>5</sup> The intent of the LandCyber framework is to ensure that the tasks, opportunities, and vulnerabilities of the cyberspace domain are addressed in the commander's concept of the operation to support the unified land commander in establishing optimal combination of effects to influence the threat before it can impact friendly forces and operations.

b. Eight aspects of convergence. Convergence is a primary force driving transformational change. The LandCyber solution framework accounts for eight aspects of convergence with significant implications for the Army.

---

<sup>5</sup> Romjue, J. (1984, May-June). *Evolution of AirLand Battle*. Air University Review.

(1) The convergence of time and space made possible by technological innovations in ICT, by which distant places move closer together in terms of the time it takes to send messages, direct or invoke action, or create effects between them.

(2) The convergence of threat with technology that empowers asymmetric advantage against modern network enabled conventional forces.

(3) The Army's constant presence in both domains as a network-enabled force reflects the convergence of the land and cyberspace domains.

(4) The convergence of the electromagnetic spectrum (EMS) and cyberspace operations is the point where cyberspace operations access the EMS to utilize code and data across wireless communication technologies and systems to enable Soldiers, units, and unmanned vehicles to operate effectively.

(5) The convergence of defensive with offensive cyberspace operations to ensure one function informs the other to assure success and mitigate unintended consequences and cyber fratricide.

(6) The convergence of the IE with cyberspace (through data and information exchange that is pushed and pulled globally into the cyberspace domain) increased the importance of cyberspace as an element of the IE.

(7) The convergence and integration of information management with knowledge management (KM) to achieve advantage in an era where large data will be leveraged by emergent "big data" analytics provide commanders at all levels with an understanding of their OEs.<sup>6</sup>

(8) The convergence of Army operational and institutional activities is occurring at an accelerating rate as they share the same cyberspace, creating an unprecedented level of interaction where operations impact institutional activities and vice-versa. Convergence leverages the speed of acquisition and fielding, and utilizes capabilities brought on by combinations of new technologies. See appendix E for institutional considerations.

c. Nine LandCyber guiding principles. The LandCyber solution framework is founded on a set of guiding principles that account for the eight aspects of convergence on Army operations, forces and the institution.

(1) Unified cyberspace operations. Land operations in the future will occur among the populace where information, influence, partnerships, and legitimacy are key enablers. Land, cyber, and human activity will continue to converge with increasing interdependence on land and cyberspace operations. The Army will develop capabilities to conduct cyberspace operations supporting ULO to maintain a decisive edge in this domain.

---

<sup>6</sup> Big data is defined loosely as a collection of data sets so large and complex that it is difficult to process using on-hand database management tools or traditional data processing applications.

(2) Integration. Integration of WfFs with operations in cyberspace will create multifunctional combined arms operations that include the land and cyberspace domains.

(a) Integration across operational and institutional echelons. The Army will have the capability to defend its own networks to maintain freedom of action in cyberspace. Through the integration of operational and institutional echelons, the evolution and maturation of command relationships will establish a formal line of authority, communications, and responsibility to oversee, coordinate, deconflict, and direct the execution of cyberspace operations at echelon. Unified land commanders require seamless time-sensitive institutional support for complex problems. See appendix E for institutional considerations.

(b) Integration across unified action partners. Army networks depend on other partner capabilities and commercial infrastructure. Through joint constructs prescribed by USCYBERCOM and the NSA, strategic partnerships will assist commanders in controlling key cyber terrain facilitating operations. In concert with USCYBERCOM, the Army will collaborate and integrate with U.S. government departments, agencies, and partners, supporting their efforts and ensuring its own ability to operate in cyberspace. This mutual assistance will include information sharing, support for law enforcement, defense support of civil authorities (DSCA), and homeland defense, undertaken only as part of a joint and interagency effort.

(c) Across functions and tasks. Cyberspace operations, consisting of tasks to build, operate, defend, exploit, and attack, will be executed from an integrated warfighting platform approved and resourced for such missions and available to support the unified land commander in achieving his objectives.

(d) Staff integration and interaction. Today, the interaction of the 2-3-6-7 and the 9 staff elements at echelon establish working environments, led by the operations officer) to facilitate unity of effort among the processes performed in the operations section, the intelligence section, the signal section and the information operations and civil affairs section. With the complexity of cyber and land operations, unity of effort will be vital to access and control key cyber terrain to meet data and information demands and to conduct the full range of cyberspace operations. Expanded interaction that fully integrates all five staff elements will offer the opportunity to address the requirements for technical, organizational, and operational execution of cyberspace operations in support of land operations. The cyber electromagnetic (CEM) element will provide the solution for the staff integration gap.

(3) Localized cyberspace effects to the tactical edge. In addition to traditional lethal and nonlethal capabilities, unified land commander will be supported, via joint constructs, with the full range of cyberspace capabilities to enable knowledge of the physical, virtual, and human dimensions of local situations, and to apply a combination of land and cyber force to shape the behavior of targets to achieve the commander's intent.

(4) Enhanced understanding. The Army will develop capabilities to build a common operational picture (COP) that identifies cyberspace opportunities, risks, and vulnerabilities in both land and cyber domains. Cyber SA will visualize the OE to provide situational understanding (SU) that supports decisionmaking in real time. The Army will win the

cyberspace reconnaissance and counter-reconnaissance fights and ensures it can conduct cross-domain operations. This requires a COP informed in real-time by blue force network systems data that provides indications and warnings to enable commanders to act, react, and counteract at network speed while simultaneously conducting informed active defense operations.

(5) Network as an operational warfighting platform and function. The future Army network will be secure, resilient, standards-based, and cloud-based enterprises fully integrated with JIE and intelligence community-information technology enterprise (IC-ITE), that will support required cyberspace capabilities; enable global collaboration; and ensure access at the point of need. Joint, interoperable, agile, flexible, resilient, and secure, the Army networks will transition to be integrated into the JIE and be an operational warfighting platform, extended to the tactical edge and capable of enabling a full range of cyberspace operations. The future cyber warfighting platform will also enable operational maneuver from a strategic distance, seamlessly leveraging Army operational and institutional forces and capabilities to prevent conflict, shape outcomes, and ultimately win, in all OEs.

(6) Combined arms approach. The generation of combat power in the cyberspace domain may be achieved by the combination of CEMA, IIA, operations security, military deception, and space into a combined arms cyberspace operations capability that supports the unified land commander. This combined arms approach will be powerful in both form and function, delivering strategic-to-tactical effects in favor of the unified land commander.

(7) Achieve cyberspace domain superiority. In concert with joint constructs, the future Army cyber force will conduct a full range of cyberspace operations enabling the unified land commander to achieve desired effects in all warfighting domains. The Army will achieve a degree of dominance that allows the conduct of cyberspace operations at a time and place of the unified land commander's choosing, to seize, retain, and exploit the initiative.

(8) Ensure mission command. Cyberspace as a linkage to all joint and service enablers is envisioned as a norm. Traditional land missions, such as critical infrastructure protection, security cooperation, and DSCA, are reliant on networks. By building, operating, and defending designated cyberspace infrastructure, Army cyber forces will enable the commander with decentralized operations, understanding of the IE, and rapid transition between operations.

(9) Empowered LandCyber units and Soldiers. LandCyber empowers units and Soldiers with land and cyber platforms to provide agile applications for joint fires and maneuver, and knowledge to maneuver physically and virtually across both domains. This approach builds knowledge of the physical, virtual, and human dimensions of the situation and applies a combination of land and cyber force to shape behavior of targets to achieve the unified land commander's intent.

### **3-4. Components of the solution and supporting ideas**

- a. Future national and strategic operational force framework

(1) USCYBERCOM national defense capability. In collaboration with the joint staff and other services, USCYBERCOM is building and organizing a cyberspace national defense capability. The framework for USCYBERCOM future operations focuses on cyberspace units built, trained, and provided by the services to conduct defense of the Nation, provide combatant command cyber contingency capabilities and operational planning, and integrate capabilities to defend DOD infrastructure.

(2) USCYBERCOM lines of operation. USCYBERCOM national and strategic cyberspace operations capabilities are divided into three lines of operation. These lines are described below.

(a) DOD information networks (DODIN) operations (DINO). DINO gains and maintains access to the cyber domain via the execution of architect (plan and engineer), build (install), configure, secure, operate, maintain, and sustain functions in and through the LandWarNet.

(b) Defensive cyberspace operations (DCO). DCO uses passive and active operations to preserve the ability to utilize friendly cyberspace capabilities and protect networks and net-centric capabilities.

(c) OCO. OCO are conducted in concert with the DINO and DCO to enable operational planners to coordinate and synergize effects in and through cyberspace and other domains to support the accomplishment of the commander's objectives.

b. Future Army operating force framework.

(1) Operationalize unified land cyberspace operations. An operational and institutional framework which supports cross functional and task synergy to integrate the CEMA, address the EMS, IO, and IIA, KM, and the human aspects of conflict is required to operate effectively in the cyberspace domain.

(2) Army cyberspace mission areas. Operational integration across CEMA, IIA, and joint IO to generate combat power in cyberspace and support national-to-tactical land operations requires four mission areas. These mission areas are described below.

(a) Cyberspace control mission area. Cyberspace control operations, enabled through the operation and defense of the Army network enterprise, provide freedom of maneuver and action within Army networks and network systems. Network operations consist of configure, secure, operate, maintain, and sustain actions that achieve agreed service levels, restore services levels to the commander's priorities, and manage incidents, problems, performance, and change. Defense includes passive and active actions taken to defend the LandWarNet and when directed, other specified cyberspace. Hunting (active defense) focuses on cyber threats not detected, mitigated, or defeated by routine system administration or other security measures. Hunting operations are performed at enterprise, regional, and local levels across the Army LandWarNet in concert with joint cyber provided constructs.

(b) Cyberspace force enhancement mission area. CEMA within the operations process, together with IO and IIA, integrate into the military decisionmaking process and orders, as part

of planning, preparation, integration, execution, assessment, and risk management activities. This series of processes maintains military advantage through SA and SU of CEMA within the OE; CEMA knowledge is created and transferred by the networks and information systems that create the COP, facilitating knowledge operations through knowledge creation and transfer.

(c) Cyberspace support mission area. The outcome in this mission area is to build a defensible network. Cyberspace support operations plan, engineer, build, and install the LandWarNet and other specified cyber infrastructure (physical and logical components) that enable end-to-end functionality. Planning is action taken to understand the situation and mission; develop, analyze, and compare courses of action for use of the network; decide a course of action that best accomplishes the mission; and produce an operation order, or order for execution. Engineering is action to design the schema of the network and information services. Building and installation is physically employing hardware and software resources to support the commander's intent.

(d) Cyberspace force application. In concert with joint constructs, Army cyberspace force application operations provide cyberspace exploit, attack, and influence capabilities to deliver effects in and through cyberspace to meet the unified land commander's intent or desired effect.

- Exploit is OCO activity, when authorized and directed, and is taken to access adversary networks, information technology, infrastructures, and associated data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Defined as an intelligence activity, exploit activity on the NSA cryptologic enterprise is strictly regulated of all activities.
- Attack is action taken, if authorized and directed by Presidential directive or EXORD, to manipulate, disrupt, deny, degrade, or destroy adversary networks, IT, infrastructures, and associated data, Internet, telecommunications networks, computer systems, embedded processors, and controllers. This is a sensitive activity, so authority for attack will flow to the Army cyber-led joint task force from USCYBERCOM.
- Influence is action taken, when authorized and directed, to manipulate or reinforce threat, adversary, or other authorized targeted human or machine security-related behavior.

(3) Future joint regional framework. USCYBERCOM envisions a seamless and integrated functional organization to address the requirement for a DOD-wide, unified and responsive effort in cyberspace. A joint cyber component command aligned to geographic combatant commanders (GCC) will provide the full range of cyber organization requirements of this vision. The Army will align its operational framework to nest with this structure.

(4) Future Army regional framework.

(a) An integrated warfighting platform. The Army possesses an array of signal, intelligence, EW, IIA, space, and KM organizations, personnel, and capabilities at echelon which will combine in synergistic constructs to provide the unified land commander with the operational edge in the cyberspace domain and on land. Signal commands (theater) will transition from Army network builders and operators into organizations with cyberspace network defense operations capabilities and subject matter expertise in all disciplines of cyberspace

planning, coordination, and deconfliction. A cyber-focused intelligence support capability will support the commander's planning and intelligence analysis in theater.

(b) Reserve component theater information operations groups. These groups could be repurposed and aligned regionally to evaluate regional information, and human aspects of conflict. Inputs and outputs from the groups integrate with cyberspace warfighting platform operations, either as part of USCYBERCOM or another structure.

(c) The JIE. The JIE will evolve and employ new technology to streamline information technology capabilities, data mining, and big data capabilities to facilitate indications and warnings, information sharing across WfFs, which includes knowledge sharing, and deconfliction. This framework will assist command staffs and units with knowledge and depth of defense, and provide new means of reconnaissance in the commanders' areas of influence and interest.

(d) Regional Army offensive cyber units. In concert with the joint constructs directed by USCYBERCOM, Army-led offensive cyber mission teams will be established and nested within USCYBERCOM and the NSA's cryptologic enterprise as part of a joint cyberspace operations construct. These teams will provide a regional focus and subject matter expertise on adversary and enemy infrastructure, and use of the cyberspace domain. These offensive cyber capabilities will answer joint force validated requests for cyber effects to create effects for the unified land commander. This approach will support decentralized planning and execution of the full range of cyberspace activities by focusing Army-led teams, operating from within the joint cyberspace operations construct on operational and tactical support requirements.

(6) Future Army tactical forces framework. At echelon, the Army has signal and intelligence companies critical to cyberspace warfighting platform. These signal and intelligence elements, if authorized and directed, could integrate and support expeditionary cyberspace operations.

(7) Localized cyber effects to the tactical edges. Cyberspace capabilities will be made available to the unified land commander, including capabilities that support proactive defense of friendly networks and systems that will assist them in sustaining operational and tactical advantage. This includes the employment of weapons platforms, such as unmanned aircraft and ground systems that rely on networks and the EMS to function. Within the joint construct supporting OCO, the ability to deny, degrade, or disrupt enemy critical communication nodes and remain cognizant of social media in the AO will be necessary.

(8) A full complement of electronic warfare (EW) capabilities. The Army will develop EW capabilities to deny opponents an actual or perceived advantage in the EMS and ensure unimpeded friendly access. Army EW will search for, intercept, identify, locate, and distinguish between sources of intentional and unintentional radiated electromagnetic energy with increased precision.

(9) IIA. The unified land commander, with the proper authorities, will aggressively shape IIA perceptions among relevant groups, such as adversaries, host nation and foreign civilian



populations, in an IE characterized by transparency and hyper-global connectivity through a virtual presence.

(10) Expanded strategic and campaign planner skills. The Army will expand excellence in military planning and policy development with broad, liberal, educational backgrounds that include life-long learning and possession of graduate degrees in strategy-related fields ( such as, history, international relations, and others), to include expertise in cyberspace policy, security, planning, and operations.

(11) In concert with Presidential and Secretary of Defense guidance, cyber forces could provide virtual presence and virtual partnerships for CONUS-based forces to allow a commander and unit to conduct activities as though present in an AOR, to give the appearance of being present, or to have an effect, via cyber capabilities, at a place other than their true location. Supported by joint directives, virtual partnership would include a set of activities conducted remotely with allies and friendly nations to build relationships that promote specified U.S. interests, build allied and friendly nation capabilities for self-defense and coalition operations, and provide U.S. forces with peacetime and contingency access.

(12) Future Reserve component.

(a) Reserve component integration. The Reserve component will use existing forces to augment Army requirements for operating in the cyberspace domain. At the strategic level, reserves can contribute specific strategic multidiscipline analysis to support the preparation of the OE through existing intelligence centers, and support the ASCCs. At the regional echelon, the Reserve component may add civil affairs, EW, IO, leader engagement, military intelligence (MI), military information support operations, and space to form combined arms capability to support phase 0 to phase 5 operations. At the operational level, the Reserve component may increase the size of units and add EW, IO, leader engagement, and MI functionality to improve existing capabilities. Theater information operations groups will repurpose structure to conduct information activities and support cyber warfighting requirements.

(b) DSCA. U.S. Northern Command, U.S. Central Command, and the Department of Homeland Security will integrate mobile Reserve component cyber build, operate and defense forces, enabling capabilities at regionally-located sites, (such as, at an Army Reserve Intelligence Support Center), to support contingency Title 10 operations for homeland defense and emergency response missions.

(c) Homeland defense. In accordance with approved joint constricts and directives, The Reserve component will establish capabilities to respond to cyber incidents in the homeland at state cyber centers. Supporting Army prevent, shape, and win roles, the Army National Guard, leveraging dual-status command and Title 32 authorities, will interface at the state and federal level to respond, secure, and remediate a secure cyberspace operating environment.

c. Future seamless operational and institutional force.

(1) The future operational force will require the ability to reach back to the institutional force to solve fast-paced emerging problem sets. In concept with joint and interagency cyber

centers, a federation of cyber models, simulations, and gaming could facilitate predictive analysis of persons, groups, threats, and other factors of interest to the unified land commander in its execution of prevent, shape, and win roles.

(2) Immediate OE and mission requirements usually consume the unified land commander who may require additional intelligence support to assist in looking at evolution in the virtual and cognitive dimensions for significant social and threat changes in the OE.

(3) Opportunities may arise in the virtual and cognitive dimensions that are not readily apparent to the unified land commander. Seamless interaction from a strategic distance with the institutional force may help find new advantages in its execution of prevent, shape, and win roles.

(4) Spectrum management, signal, intelligence, EW, space, KM, and the human aspects of conflict will require a seamless operational and institutional unified effort, informed by current operations, to manage the integration of these parallel capabilities. Detailed institutional force considerations in support of the operational force are provided in appendix E.

---

## **Chapter 4**

### **Army WfFs, Human Aspect of Conflict, and Cyberspace Capabilities**

#### **4-1. Introduction**

a. America's ability to deter threats against, and to operate from, declared areas of hostility is critical to conducting global military missions and to defend the U.S. homeland.

b. Within joint constructs of land and cyberspace operations, commanders use the WfFs to exercise command and their staffs to exercise control.<sup>7</sup>

c. The following sections address common cyberspace capabilities and describe the unique cyberspace capabilities the WfFs will depend upon for their systems and tasks.

#### **4-2. Cyberspace capabilities across WfFs**

a. LandWarNet. In the future OE, Army forces from the strategic to the tactical level will require access to protected cyberspace and the capability to withstand or mitigate the effects of jamming and deliberate interference. LandWarNet, as the unified land commanders protected terrain cyberspace, will be able to withstand or mitigate the effects of jamming and deliberate interference through a single, secure, standards-based, versatile infrastructure,. LandWarNet is linked by networked, redundant, transport systems, sensors, warfighting and business applications, and data, to provide Soldiers and civilians the information they need, when needed, in any environment, to enable decisive actions with unified action partners.

---

<sup>7</sup> ADP 3-0, p 13.

b. Standardized network configuration management. The lack of a single network standard across AORs and a single entry point into the network enterprise presents configuration management and network standardization challenges that impact mission accomplishment.

c. Network operations (NETOPS). NETOPS consists of enterprise management, network assurance, and content management capabilities. NETOPS are critical to all WfFs, as they provide operational, organizational, and technical capabilities for operating and defending Army, JIE, and other specified cyberspace.

d. Hunt. Army organizations, in concert with joint cyberspace protect concepts, will require the capacity to meet current active cyber defense persistent threat hunting, security inspection, vulnerability assessment, and remediation mission requirements in support of commanders.

e. EMS. Increased military reliance on electronic attack and electronic protection, the rapid expansion of commercial technology, the proliferation of unmanned aerial systems, and the expanding demand for wireless technology will complicate requirement to manage EMS. Continued uncontrolled acquisition of non-program of record commercial devices introduced into Army formations and theater of operations with a crowded EMS, and a growing demand for full, on-demand, real-time video and data at all echelons increases risk to military operations.

f. Information sharing. Information sharing among networks is conducted via manpower intensive methods that introduce viruses and data spillages. In concert with JIE and IC-ITE information sharing constructs, new cross-domain technologies are needed to automatically and securely transfer information among Internet protocol networks. The transition of information between WfFs to support operations will be seamless.

g. Tactical radio and other personal electronic devices. Increasingly, a variety of digital devices will be introduced at the tactical edge. Most of these devices are networked and require an Internet protocol address to communicate. These devices will utilize common or tailored applications, pulling or pushing information. Many of these devices will give tactical formations greater reach, improved agility, quickness, and physical environment SA. However, a major challenge will be finding a means to increase the Soldiers' cyberspace SA. Cyberspace is largely transparent and rarely conveys warnings to traditional human senses when under attack from cyberspace. The stealth and speed of cyberspace will require new training, skills, and understanding by Soldiers.

h. Robotics and intelligent grid arrays. Robots are utilized progressively more by the Army to mitigate risks and obtain advantage. Unmanned aerial and ground systems connected to an extensive network will enhance friendly forces' SA and tactical reach in ways not previously possible. Capabilities in the future will provide smart grid arrays. These intelligent arrays will be networked devices designed to perform anti-access or area denial missions for tactical formations. An echelon's tactical operations center or local security command post will operate intelligent arrays. There will be intelligent networked capabilities that provide visual, signature or movement warning for local security and perimeter defense. Soldiers and robots will be equipped with devices and systems with blue force tracking functionality that enables the ability to move unencumbered through defensive zones. Sensors will interrogate and identify Soldiers

and robots moving through the area without such a device for evaluation as a potential adversary. Such capabilities will preserve combat power and increase survival for other critical mission tasks.

i. Mission command unique.

(1) The execution of the four cyberspace mission areas outlined in chapter 3 is accomplished under the integrating construct of mission command. A fully integrated combined arms-like approach using CEMA, IIA, and intelligence capabilities will be essential to the accomplishment of these mission areas.

(2) Cyberspace SA and the COP. The unified land commander requires SA to create effects in cyberspace. Consequently, a cyberspace COP must be dynamic and interactive, and provide tailored detail to comprehend fully the consequences of cyberspace operations. This COP integrates with the mission command COP. Future mission command systems will enable the receipt and dissemination of relevant information from the dismounted Soldier and from disparate information and intelligence systems to all command posts for display on the COP. This system attribute supports cyberspace visualization, enhanced collaboration, shared understanding, effective coordination, and synchronized action.

(3) OCO. In concert with joint prescribed constructs for OCO, the availability of expeditionary OCO capability to the unified land commander will be required. The unified land commander will encounter adversary and enemy networks that give them a distinct advantage over Army forces and systems. Closed and dark networks will hinder U.S. national technical means of discovery in advance of ground operations.<sup>8</sup>

(4) Strategic cyberspace planner development. Educate to expand analytical and problem solving skills as applied to strategists and planners in the cyberspace domain. Integrating land and cyberspace will broaden their abilities to conceptualize rapidly and develop creative feasible solutions to complex challenges. Enable these experts to convey succinctly complicated cyberspace conceptual or analytical material in a manner that is understood clearly by decisionmakers.

j. Movement and maneuver unique.

(1) The unified land commander will move and maneuver simultaneously inside the land and cyberspace domains. Today's threats recognize that directly engaging traditional Army forces is not practical. The preferred alternative is to fight Army forces asymmetrically to include in and through the cyberspace domain. The Army often moves through the cyberspace domain without seeing or understanding the implications and risks. The provision of CEM elements helps address this shortfall; however, the picture is still incomplete. Consistent with joint constructs, the unified land commander requires the capability to reach and engage adversaries and enemies in cyberspace. This requires Army forces to see its force status, capabilities, and data along with that of friendly, neutral, and adversary forces as well as actors

---

<sup>8</sup> Closed networks are not connected to the greater Internet. Dark networks are connected to the greater Internet but hidden and inaccessible through normal means.

within the cyberspace domain. The ability to provide specific and authenticated information on Army forces and capabilities coupled with predictive analysis on intentions and capabilities of friendly, neutral, and, adversary forces, and actors within the cyberspace domain is a critical enabler.

(a) Offensive and defensive cyber operations are most critical as the unified land commander maneuvers to defeat the enemy. Current maneuver formations lack the ability to counter a wide-area or local cyber-attack.

(b) Future unified land commanders will be supported sufficiently to a cyber attack and to defeat the attack whether on the move or stationary.

(2) Commanders must be trained effectively on cyber operations to plan for, request, and integrate cyber capabilities and effects into operational plans and schemes of maneuver. Adversaries and enemies will challenge the future unified land commander in the land and cyberspace domains, simultaneously requiring commanders to synchronize cyberspace and land operations.

(3) Rebuilding critical infrastructure after destruction by U.S. forces is expensive. Rebuilding creates other challenges, such as re-establishing governance, economy, power, basic services, and free press, when there is no supporting infrastructure. DCO and OCO will reduce loss of life and facilitate preservation of infrastructure. There will also be instances where the unified land force will encounter adversary networks which, if not engaged in and through cyberspace, will cause hardship and loss of life. Cyberspace operations provide a positional advantage by adding additional avenues of approach against enemies.

k. Intelligence unique.

(1) Dedicated and reinforcing intelligence support is essential to the accomplishment of the four cyberspace operations mission areas: cyberspace operations control, cyberspace operations force enhancement, cyberspace operations support, and cyberspace operations force application.

(2) Intelligence, surveillance, and reconnaissance collection in joint operations. The unified land commander lacks cyberspace-based surveillance and reconnaissance systems beyond traditional ground, air, and space-based systems to provide critical support to the operations process. Supporting intelligence capacity nested in the joint cyberspace operations and intelligence enterprise will enable SA and provide commanders with the opportunity to conduct decentralized operations over extended distances with expanded capabilities.

(3) The intelligence WfF is in a position to transform the Army and its use of cyberspace by developing and providing threat analysis of cyberspace, and informing other WfF operational plans and schemes of operation. Adversaries and enemies will challenge commanders in at least two domains simultaneously, so commanders need a capability that seamlessly connects and integrates the full range of Army cyberspace operations with a cyber-integrated intelligence preparation of the battlefield and a threat overlay.

(4) Army leaders rely extensively on intelligence to execute missions. The capability for supporting physical operations is at risk if the network is not available to contrast the friendly force situation with an informed picture of land and cyberspace threats.

(5) EW capabilities require Intelligence. EW capabilities will evolve in response to the threat and the U.S. use of the cyberspace domain and the EMS. Intelligence is essential to the CEMA process to inform the commander's scheme of maneuver.

(6) Intelligence is critical to the planning and provision of offensive cyberspace capabilities. Extensive OPE when authorized and directed, is required to develop the SA necessary to conduct cyberspace operations and relies heavily on intelligence to inform cyberspace operations via its integration with and leveraging of the global cryptologic enterprise.

(7) The provision of intelligence formations and capabilities, and offensive cyberspace teams and capabilities, is critical to enabling the unified land commander to fight in land and cyberspace domains simultaneously. Intelligence enables Army-led Joint Force Headquarters (cyber) (JFHQ-C) to facilitate remote cyberspace operations for use against threats connected to the internet. For threats not connected directly to the internet, the "air gap" must be bridged by the appropriate technologies and capabilities, potentially with deployable expeditionary cyberspace teams.<sup>9</sup>

(8) Intelligence is an essential element supporting CEMA. Both activities must plan and incorporate cyber offensive operations and the EMS into the commander's scheme of maneuver.

#### 1. Fires unique.

(1) Integration of CEMA into the joint targeting process optimizes and integrates the commander's capabilities and ensures proper synchronization and deconfliction of effects. Failure to incorporate CEMA into operations will cede this domain to the enemy and may lead to a longer, more costly mission, and negative social perceptions.

(2) In concert with joint constructs, the emergence of electric fires and the introduction of similar directed electromagnetic energy efforts to the unified land commander will create circumstances that introduce new vulnerabilities and advantages, including vulnerabilities to the LandWarNet. Partnering with the fires and space communities as these technologies mature will be critical to the preservation of LandWarNet capabilities and the effective use of the full range of electronic fires.

(3) Joint fires coordinates and synchronizes organic intelligence assets and nonlethal effects in support of the commander's objectives through the targeting process. This process will evolve with increasing threat and the U.S. use of the cyberspace domain and the EMS. Fires is integral to CEMA; CEMA is integral to targeting board operations. Both plan and incorporate cyberspace capabilities into the commander's scheme of maneuver.

---

<sup>9</sup> An air gap is a security measure ensuring that a secure network is physically isolated from insecure networks, such that there is no ability for computers on opposite sides of the air gap to communicate.

m. Sustainment unique.

(1) The Army will develop the capability to rapidly acquire and upgrade network infrastructure and systems, and leverage new technologies. The Army will also deliver cyber infrastructure, consistent with the joint force construct, to extend operational reach and sustain cyberspace operations.

(2) Sustainment incurs additional risk to its operations, data, information, and the DODIN due to its reliance on networks, organizations, partners, industry, and academia that operate primarily in the unclassified environment and exist outside of the DOD infrastructure and influence.

(3) Army information systems are vulnerable to tampering at the points of design, manufacture, service, distribution, and disposal. Safeguards will be employed within the supply chain to ensure trusted platforms. Partnerships with industry and providers are critical to mitigating risk.

n. Protection unique.

(1) The number of devices connected to the Army network at the tactical edge will continue to grow and empower leaders and warfighting formations. However, these devices are often wireless and commercial off-the-shelf, thus introducing added risk to providing protection. Proper use, accountability, configuration, and management of these devices are critical to the overall protection of the Army.

(2) Protection is an integral part of CEMA. The CEM environment requires working groups to plan and incorporate cyberspace protection into the commander's scheme of maneuver.

(3) Physical security and operations security, will account for threats across the range of cyberspace operations, including infrastructure.

#### **4-3. The human aspect of conflict in cyberspace**

Warfare centered on defeating adversaries cloaked as cyberspace personas places a rising premium on conventional and special operations forces' ability to consider the human aspects of conflict and cyberspace operations. Conflicts in cyberspace require exceptional SA and SU due to the nature of the operations. In some cases, a profound understanding of foreign culture, foreign languages, intelligence capabilities, use of diplomatic means, Army foreign area operations, IIA, cyberspace operations, and civil affairs operations is required.

#### **4-4. Summary**

Cyberspace capabilities provide the tools that enable operational adaptability and extend the power of joint cyberspace capabilities to the tactical edge. Cyberspace operations training and leader development support the cognitive component that links capabilities to the operations process and results in the delivery of cyberspace operations services and effects. Achieving the Army's vision for cyberspace operations requires the Army to participate actively in defining and developing needed cyberspace capabilities. Specific required capability statements derived from the preceding discussion are provided in appendix B.

---

## **Chapter 5**

### **Conclusion**

a. This white paper describes Army cyberspace operations, needs, and joint required capabilities in the 2018-2030 timeframe, consistent with Joint Pub 3-12. It builds upon the joint guidance and direction expressed across a range of conceptual and doctrinal frameworks. The paper describes the relationship between the Army WfFs and operating in the cyberspace domain.

b. While the DOD is a critical contributor to helping mitigate strategic risk and protecting the nation's interests, the services and the unified land commander in particular, face operational and tactical threats from cyberspace. Failure to achieve freedom of maneuver in the cyberspace domain will result in operational risk. Ultimately, the failure to organize, concentrate, and integrate cyberspace operations functions and tasks places Army forces at significant risk and disadvantage on land, and as a land power.

c. This white paper describes a transformational concept that deals with emerging cross-domain dynamics, land and cyberspace, accounts for fundamental changes in the OE and acknowledges that commanders operating in cyberspace are governed by laws, policies, regulations, and rules of engagement that must be understood and considered in planning, coordinating, and executing cyberspace operations.

d. The Army must think globally and act locally in the cyberspace domain, in concert with land forces and the human dimension, to shape the physical and virtual behavior of human populations and machines to its opportunity and advantage. The Army must become organized, trained, and equipped to shape human behavior on land and in cyberspace to keep pace with the emergence of a virtual domain that has moved activity relevant to land operations outside the traditional AOs of armies.

d. LandCyber is a solution framework that accounts for eight areas of convergence, and is guided by nine principles outlined in this paper that deliver an integrated warfighting platform and function to enable success in the Army's prevent, shape, and win roles. A future institutional force framework to complement this white paper is provided in appendix E to assist and inform TRADOC and ARCIC cyber efforts.

---



## **Appendix A References**

### **Section I**

#### **Required References**

This section contains no entries.

### **Section II**

#### **Related References.**

Army regulations, Department of the Army pams, field manuals (FM), Army doctrine and reference publications (ADP / ADRP), and DA forms are available at Army Publishing Directorate Home Page <http://www.usapa.army.mil>. TRADOC publications and forms are available at TRADOC Publications at <http://www.tradoc.army.mil/tpubs>. Joint publications (Pubs) and directives are available at <http://www.dtic.mil> or <https://jdeis.js.mil/jdeis/index.jsp?pindex=0> Some DOD pub are available at <http://www.defense.gov/>

ADP 1

The Army

ADP 3-0

Unified Land Operations

ADRP 3-0

Unified Land Operations

ADRP 6-0

Mission Command

Capstone Concept for Joint Operations: Joint Force 2020

DOD Cyberspace Policy Report. (2011, November). A report to Congress pursuant to the National Defense Authorization Act for FY 2011, Section 934. Retrieved from <http://www.defense.gov>

DOD Directive 4630.5

Interoperability and Supportability of Information Technology and National Security Systems. (2004, May 5). [Certified current as of 2007, April 23.] Retrieved from <http://www.dtic.mil>

DOD Directive 5100.20

National Security Agency/Central Security Service. (2010, January 26). Retrieved from <http://www.dtic.mil>

DOD Directive 8500.01E

Information Assurance. (2002, October 24). [Certified current as of 2007, April 23]. Retrieved from <http://www.dtic.mil>

DOD Instruction 3305.09

DOD Cryptologic Training. (2013, June 13). Retrieved from <http://www.dtic.mil>

DOD Instruction 8410.02

NETOPS for the Global Information Grid. (2008, December 19). Retrieved from <http://www.dtic.mil>

DOD. Joint Operational Access Concept, Version 1.0

DOD. (2005, June). Strategy for Homeland Defense and Civil Support. Retrieved from <http://www.defense.gov>

DOD. (2011, July). DOD Strategy for Operating in Cyberspace. Retrieved from <http://www.defense.gov>

DOD. (2012, January). Sustaining U.S. Global Leadership: Priorities for 21<sup>st</sup> Century Defense. Retrieved from <http://www.defense.gov>

DOD. (2011, September 6). Information Technology Enterprise Strategy and Roadmap. Version 1.0. Retrieved from [http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed\\_ITESR\\_6SEP11.pdf](http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf)

DODI O-3115.07

Signals Intelligence. Change 1 (2010, November 19). [Password protected. Available through [www.dtic.mil](http://www.dtic.mil)]

EXORD 155-10 with FRAGO 1. Army cyberspace operations and the establishment of an end state United States Army Cyberspace Command. (2010, September 30). September 2010. Retrieved from <http://exprdev1.dca.expr.net/obfweb>

Executive Order 12333: United States Intelligence Activities.(1981, December4). Retrieved from <http://www.archives.gov/federal-register/codification/executive-order/12333.html>

FM 6-02.70

Army Electromagnetic Spectrum Operations

FM 6-02.71

Network Operations. [Password protected. Available through AKO access only.]

FM 2-01.3

Intelligence Preparation of the Battlefield/Battlespace. [Password protected. Available through AKO access only.]

FM 2-19.4

Brigade Combat Team Intelligence Operations. [Password protected. Available through AKO access only.]

FM 2-22.2

Counterintelligence. [Password protected. Available through AKO access only.]

FM 2-91.6

Soldier Surveillance and Reconnaissance Fundamentals of Tactical Information Collection. [Password protected. Available through AKO access only.]

FM 3-13

Inform and Influence Activities

FM 3-55

Information Collection

FM 3-60

The Targeting Process

FM 6-02.70

Army Electromagnetic Spectrum Operations

FM 6-02.71

Network Operations. [Password protected. Available through AKO access only.]

Headquarters DA General Order No. 2010-26

Establishment of U.S. Army Cyber Command. (2010, October 1). Retrieved from <http://armypubs.army.mil/epubs/pdf/go1026.pdf>

International Strategy for Cyberspace – Prosperity, Security, and Openness in the Networked World. (2011, May). Retrieved from [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)

Joint Operational Access Concept. Version 1.0

Joint Pub 2-01

Joint and National Intelligence Support to Military Operations

Joint Pub 2-01.3

Joint Intelligence Preparation of the Operational Environment

Joint Pub 3-0

Joint Operations

Joint Pub 3-13

Information Operations

Joint Pub 3-13.1  
Electronic Warfare

Joint Pub 3-14  
Space Operations

Joint Pub 3-60  
Joint Targeting

Joint Pub 5-0  
Joint Operations Planning

Joint Pub 6-0  
Joint Communications System

Joint Pub 6-01  
Joint Electromagnetic Spectrum Management Operations

National Security Space Strategy. [Unclassified summary]. (2011, January). Retrieved from [http://www.defense.gov/home/features/2011/0111\\_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary\\_Jan2011.pdf](http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf)

National Security Strategy. (2010, May). Retrieved from [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf)

National Security Council Intelligence Directive 6 (NSCID 6). (1947, December 12). Foreign Wireless and Radio Monitoring. Retrieved from <http://history.state.gov/historicaldocuments/frus1945-50Intel/d424>

NSA Association. General Council Memorandum: Access to Foreign Intelligence Surveillance Act Data. [Classified]. (2012, May 8). [This publication is not available without clearance and authorization. For authorized personnel, contact: National Security Agency, Attention: Office of General Council (Intelligence Law), 9800 Savage Road, Fort George G. Meade, MD 20755-6000.]

Director, NSA Memorandum. (2013, June 11). Delegation of Signal Intelligence to USCYBERCOM. [Classified]. [This publication is for official use only and only available through proper clearance and authorization. For authorized personnel, contact Commander, USCYBERCOM, Attention: J55 Policy and Doctrine, 9800 Savage Road, Fort George G. Meade, MD 20755.]

Presidential Policy Directive-20: U.S. Cyber Operations Policy; [Classified]. (2012, October). [This publication is not available without clearance and authorization. For authorized personnel, contact Commander, USCYBERCOM, Attention: J55 Policy and Doctrine, 9800 Savage Road, Fort George G. Meade, MD 20755.]

Romjue, J. L. (1984, May-June). *The Evolution of AirLand Battle*. Air University Review. Retrieved from <http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/may-jun/romjue.html>

Secretary of Defense. Memorandum for Secretaries of the Military Departments (2009, June 23). Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations. Retrieved from <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-029.pdf>

The National Military Strategy of the United States of America. Redefining America's Military Leadership. (2011, February 08). Retrieved from [http://www.jcs.mil/content/files/2011-02/020811084800\\_2011\\_NMS\\_-\\_08\\_FEB\\_2011.pdf](http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf)

The National Military Strategy for Cyberspace Operations. (2006, December). Retrieved from [http://www.dod.mil/pubs/foi/joint\\_staff/jointStaff\\_jointOperations/07-F-2105doc1.pdf](http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf)

TRADOC Operational Environments to 2028: The Strategic Environment for Unified Land Operations

TRADOC. (2013, July 9). The Enabling Operations in Cyberspace through Institutional and Operational Unity of Effort White Paper. [password protected. Available by request from proponent.]

TRADOC Pam 525-2-1

The United States Army Functional Concept for Intelligence 2016-2028

TRADOC Pam 525-3-0

The U.S. Army Capstone Concept

TRADOC Pam 525-3-1

The U.S. Army Operating Concept 2016-2028

TRADOC Pam 525-3-3

The U.S. Army Functional Concept for Mission Command 2016-2028

TRADOC Pam 525-3-4

The U.S. Army Functional Concept for Fires 2016-2028

TRADOC Pam 525-3-5

The U.S. Army Functional Concept for Protection 2016-2028

TRADOC Pam 525-3-6

The U.S. Army Functional Concept for Movement and Maneuver 2016-2028

TRADOC Pam 525-3-7

The U.S. Army Concept for the Human Dimension in Full Spectrum Operations 2015-2024

TRADOC Pam 525-4-1  
The U.S. Army Functional Concept for Sustainment 2016-2028

TRADOC Pam 525-7-4  
The U.S. Army's Concept Capability Plan [for] Space Operations 2015-2024

TRADOC Pam 525-8-2  
The U.S. Army Learning Concept for 2015

TRADOC Pam 525-8-3  
The U.S. States Army Training Concept 2012-2020

TRADOC Pam 525-7-8  
Cyberspace Operations Concept Capability Plan 2016-2028

---

## **Appendix B**

### **Required Capabilities (RCs)**

#### **B-1. Introduction**

a. This appendix describes the Army's cyber operations RCs. The capability statements are designed to be used in the Army Concept Framework, and integrate into the Army Campaign of Learning (Army 2020, Unified Quest, and others). The capabilities are derived from select joint and Army concepts, and chapter 4 of this white paper. RCs are consistent with national and DOD policies and guidance, and joint constructs.

b. The capability statements are organized using the cyber mission areas. The cyber required capability statements will inform a cyber CBA and future required capabilities development efforts by the Army's warfighting centers of excellence (CoEs). As an endstate, the Army must develop, field, and sustain required capabilities in an incremental manner to ensure the Army has the capabilities it needs to conduct ULO successfully.

#### **B-2. RCs**

a. The Army requires the capability to build, operate, defend, exploit, and attack within, through, and from cyberspace and the EMS as part of a joint construct to detect, deny, degrade, disrupt, and destroy enemy and adversary cyberspace capabilities and activities to support unified action

b. The Army requires the capability to establish secure networks as a part of the joint and Army information enterprise, transmitting data at multiple levels of classification, to include unified action partner classifications, to provide support to unified action.

c. The Army requires the capability to provide global, secure, adaptive and rapid access with trusted and authenticated domains, at multiple levels of classification to all authorized entities

requesting interaction with resources from any location, at anytime to provide support to unified action.

d. The Army requires the capability to operate networks as a part of the JIE securely to provide end-to-end assured management of faults, configurations, allocations, performance, and security to support all Army WfFs in unified action.

e. The Army requires the capability to integrate with unified action partner networks securely during garrison and deployed operations, including those partner networks with different intelligence sharing relationships, to enable unified action.

f. The Army requires the capability to defend Army provisioned and installed data, hardware, software, networks, and network-centric capabilities at multiple levels of classification, to include unified action partner classifications in response to cyberspace threats to provide support to unified action.

g. The Army requires the capability to discover, deliver, and store data with multiple levels of classification securely, to include unified action 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 in support of unified action.

h. The Army requires the capability to govern and provide policy, development oversight, deployment, standardization, and overall management of solutions that provide generation, deconfliction, and distribution of solutions at any level in the enterprise network hierarchy to support unified action.

i. The Army requires the capability to perform threat-based security and vulnerability assessments to support Army information networks, offensive and defensive cyberspace operations and associated activities to support unified action.

j. The Army requires the capability to perform cyber site exploitation and forensics to support information networks, offensive, and defensive cyberspace operations and associated activities to support unified action.

k. The Army requires the capability to conduct, synchronize, deconflict, coordinate, and support counterintelligence, law enforcement, and expeditionary information operations to support civil authorities, homeland defense, information networks, offensive, and defensive cyberspace operations and associated activities in unified action.

l. The Army requires the capability to develop the commander's overall cyberspace and EMS SA to support mission command, and to allow for commanders and staffs to monitor the elements of critical infrastructure and key resources at both garrison and expeditionary locations supporting unified action.

m. The Army requires the capability to provide commanders with near-real-time awareness and understanding of an adversary's capabilities, plans, intentions, actions, and impact upon networks, services, systems, mission, and force, to assist in the mitigation and response to those actions as part of defensive and offensive cyberspace operations in support of unified actions.

n. The Army requires the capability to develop and provide real-time awareness and understanding of a commander's units' networks, services, and systems and the potential impact(s) on mission and force in support of unified action.

o. The Army requires the capability to provide the commander with awareness and understanding of the legal considerations, intelligence gain and loss, and risks associated with decisions, and actions taken in or through cyberspace and the EMS in support of unified actions.

p. The Army requires the capability to provide the commander with an awareness and understanding of the social layer of networks in support of the execution of information tasks and unified action.

q. The Army requires the capability to gain and maintain SA and SU across the cyberspace domain and EMS to enable integration of cyberspace with other operational domains and all warfighting functions.

r. The Army requires the capability to provide the commander with near real-time awareness and understanding of the effects of offensive cyberspace operations on adversary networks, services, and systems.

s. The Army requires the capability to establish secure networks as a part of the JIE at multiple levels of classification, to include unified action partner classifications, to provide support to unified action.

t. The Army requires the capability to engineer, construct, operate, and sustain an Army offensive enterprise to support defensive and offensive cyberspace and their associated activities, to gain and maintain friendly freedom of action, ensure friendly mission command while deny the same to enemies and adversaries to support unified action.

u. The Army requires the capability to research, develop, engineer, acquire, and deploy solutions in a time-sensitive manner to support and enable effective cyberspace operations and associated activities in support of unified action.

v. The Army requires the capability to conduct legal, regulatory, and policy analysis and coordination to support information networks, defensive and offensive cyber operations, and associated activities at echelon to support unified action.

w. The Army requires the capability to mitigate, remediate, develop, and deploy solutions to cyber intrusion or attacks to support unified action.



x. The Army requires the capability to develop access to conduct defensive and offensive cyberspace operations and associated activities, to detect, disrupt, deny, degrade, destroy and exploit enemy and adversary cyberspace and EMS systems and associated capabilities to gain and maintain friendly freedom of action, ensure friendly mission command and deny the same to enemies and adversaries during unified action.

y. The Army requires the capability to conduct dynamic cyber defense, DCO response actions, OCO, and associated activities to detect, disrupt, deny, degrade, destroy, and exploit enemy and adversary cyberspace, EMS systems, and associated capabilities to gain and maintain friendly freedom of action, ensure friendly mission command and deny the same to adversaries during unified action.

z. The Army requires the capabilities and authorities to collect, analyze, and exploit, intelligence from enemy and adversary cyberspace and EMS facilities, platforms, sensors, systems and networks to gain and maintain friendly freedom of action, ensure friendly mission command while denying the same to adversaries during unified action.

aa. The Army requires the capability to process and analyze cyber and EMS information on adversary networks to gain and maintain friendly freedom of action, ensure friendly mission command while denying the same to enemies and adversaries during unified action.

bb. The Army requires the capability to attack enemy and adversary facilities, platforms, sensors, systems, networks, critical infrastructure, key resources, and information to deny, degrade, disrupt, or destroy enemy and adversary capabilities and actions to gain and maintain friendly freedom of action, ensure friendly mission command while denying the same to enemies and adversaries during unified action.

---

## **Appendix C**

### **Facts and Assumptions**

#### **C-1. Facts**

a. Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space.

b. Effective unified action requires Army leaders who understand, influence, and cooperate with unified action partners.

c. Threats will attempt to isolate and defeat U.S. tactical formations while avoiding battle under unfavorable conditions.

d. To seize, retain, and exploit the initiative, Army forces strike the enemy lethally and nonlethally, using a joint construct, in time, places (including cyberspace), or manners for which the enemy is not prepared.

e. Homeland defense against cyberspace threats requires simultaneous and continuous application of deter and defeat at a safe distance efforts in coordination with designated civil authorities.

f. Cyberspace effects are created throughout friendly, neutral, and adversary cyberspace.

g. Future adversaries will contest joint warfighter cyberspace superiority and attempt to establish their own cyberspace superiority, within the DODIN and the whole of the domain.

h. The technology supply chain will be threatened in the form of malicious tampering with software and hardware before they are integrated into an operational system.

## **C-2. Assumptions**

a. In the future, U.S. forces will operate in environments where access to and use of cyberspace and the electromagnetic environment is increasingly challenged by a widening set of state and non-state actors.

b. Cyberspace will continue to increase in importance as part of the human aspect of conflict.

c. Significant advantage in future operations will go to the side that can command access to and use of cyberspace and the electromagnetic environment.

d. Army networks will be consistent with joint constructs, built and operated as warfighting platforms focused on sustaining freedom of maneuver.

e. The Army will require cyberspace and electromagnetic capabilities consistent with the joint cyberspace operations construct for DCO, remote and close-access OCO, and offensive EW operations.

f. USCYBERCOM will establish a joint cyber presence in each GCC's AOR within the 2014-2018 timeframe.

g. USCYBERCOM will task ARCYBER and/or JFHQ-C to provide an increasing number of offensive and defensive cyberspace forces and capabilities to support GCCs and functional combatant commands as part of a joint organizational construct.

h. Army forces will still have a responsibility to extend and defend network and information service capabilities, especially during phases 2 and 3 of operations, even though a joint network will improve interoperability through common standards and technologies.

i. The ARCYBER and/or JFHQ-C will receive EXORD direction, consistent with joint doctrine and EXORDs, through USCYBERCOM, with appropriate authorities and rules of engagement to conduct cyberspace operations in support of the joint warfighter and committed Army forces in the area of hostilities.

- j. Targets developed through cyberspace and the EMS will be critical to prevent escalation of conflict and shape future operations.
  - k. Future military operations, to include CEMA , may span multiple GCC AORs with global, regional, and localized CEM contests.
    - l. The Army will not turn off the network.
    - m. The Army will not invest extensively in electromagnetic tempering and hardening, due to prohibitive costs.
    - n. The Army will develop the LandWarNet as a defensible weapons platform consistent with JIE constructs.
    - o. Army cyberspace and the electromagnetic capabilities and operations are increasingly joint. The services will continue to introduce decision, support, weapons, training, education, and experimentation systems with integrated circuits and software fostering convergence of existing organizations and capabilities while simultaneously introducing new forms of organizations and capabilities.
- 

## **Appendix D**

### **Implications and Risks**

#### **D-1. Implications**

- a. The Army will have to repurpose and remission existing institutional organizations and operational forces.
- b. Army LandWarNet and cyberspace operations are increasingly joint and integrated with interagency organizations.
- c. The convergence of land and cyber domains place increasing demands on the LandWarNet and JIE to deliver full range capability and effects to the unified land commander.
- d. CEMA training enablers and support systems are required for units to train as they fight during collective training and unit exercises.
- e. LandWarNet will become a warfighting platform that requires it to become a program of record and pacing item consistent with JIE technical requirements.
- f. Traditional combat support will function like combat arms activities to provide a combined arms approach to generate the full range of effects in and through cyberspace.<sup>10</sup>
- g. Acquisition needs to evolve to leverage the rapid pace of technology development.

---

<sup>10</sup> The current definition of combat arms requires modification to capture this implication.

h. Commanders at all echelons will be educated on the rules of engagement as they apply to cyberspace and a theater of operation.

i. Centralized governance of the JIE must increase as DOD and the services transition to a single network to facilitate end-to-end defense and SA.

j. The JIE must continue to answer and be responsive to the direction of the commander.

k. Adversaries will develop means and capabilities to leverage cyberspace for use in all phases of operations to the detriment of U.S. operations across the elements of national power.

## **D-2. Risks**

a. If the Army does not adopt an approach for integrated land and cyberspace operations, then risk exists in the following areas.

b. Commanders' critical information requirements in support of ULO will not be met.

c. Institutional inertia will impede horizontal integration and formation of a combined arms capability.

d. SA capabilities that synergize the cyberspace and land domains will not be fielded.

e. The Army will not recruit, train and retain the Soldier and civilian cyberspace combined arms team.

f. The commander cannot realize the benefits and advantage of cross-domain synergy over adversaries.

g. Unified action partners may be unable to conduct or unwilling to contribute to the execution of cyberspace operations.

---

## **Appendix E**

### **Future Army Institutional Force Framework**

a. Below are institutional force considerations for follow-on work to adapt the Army to full range cyberspace operations in the cyber domain.

b. Functional integration.

(1) Cyberspace operations are enablers for mission command, other WfFs, intelligence, and reconnaissance, and they also provide an opportunity for deliberate mass confusion, and strategic to tactical disruption. The convergence of the land and cyber domains, network provisioning and operations, and defensive and offensive cyberspace operations are driving increased

requirements for integration of institutional and operational functions, capabilities, and organizations.

(2) To account for institutional impacts resulting from the convergence of the land and cyber domains, the Army institution must address the risks, opportunities, and tasks of cyberspace operations beyond the provision of basic network and telecommunications services. The operational and technical functional capabilities of signal, intelligence, EW, EMSO, space, and KM, and their affects on the human aspect of conflict, and the requirement for a unified effort all have institutional ramifications. The dynamics of these functions and the evolving joint organizational construct and policy environments will compel the Army to consider how best to organize institutionally to ensure fullest integration.

c. Integrated CoE. An Army cyberspace CoE will serve as the TRADOC force modernization proponent for cyberspace to achieve unity of effort for cyberspace combat developments and the force modernization process. The CoE will bring cyberspace related functions, oversight, integration, and leader development together ensuring the effective and efficient combination and integration of functions, while reinforcing unique requirements and capabilities.

d. Integrated programs analysis and resourcing. The Army may consolidate, realign, or establish new program elements, program evaluation groups, and management decision packages currently associated with the full scope of acquisition, logistics, and technology. The Army staff will lead the development of a science and technology (S&T), research, development, and acquisition strategy to provide a basis for the agile acquisition process.

e. Agile acquisition process. Much like the acquisition process supports the intelligence community, the development of an agile and responsive cyberspace acquisition process to meet the cyber threat is critical. The need for agility is most obvious at the point where the tools needed for the job are delivered and extends down through the entire chain from the delivered products to S&T. This agility requires enhanced and synchronized cyberspace materiel capabilities for a responsive enterprise across S&T, research, development, and acquisition communities. In Partnership with USCYBERCOM and NSA, the communities will provide the next generation of technology, developing, delivering, sustaining, and maintaining timely materiel solutions for the operational force. Maintaining a technical edge in the cyberspace environment in the face of agile and innovative adversaries requires dynamic identification of requirements and delivery of capabilities that include a technical solutions and trained operators.

f. Future Army cyber leader development, education, and training.

(1) The design and implementation of cyber-related leader development, education, and training will consider, to the extent practicable, the inherent joint nature of cyberspace operations and training, and the way people communicate and learn in current and future digital generations. Connecting the mission command systems in garrison, as that when deployed, will enhance leader and Soldier proficiency in core warfighting functional competencies supporting combined arms maneuver and wide area security. Providing access to training from post, camp, and station, through virtual training and cyber ranges, will impact the learning domain significantly.

Achieving a common educational platform integrated with the joint cyberspace training enterprise to provide adaptable environments to develop and enhance individual skills will benefit force growth.

(2) In concert with USCYBERCOM directives, the integration of a WCCO into the Army training center framework is critical to preparing forces for future missions. This effort will include subject matter expertise imbedded within the mission command training program, pre-command programs, Army senior, advanced, and basic training courses for officers, warrant officers, noncommissioned officers, and enlisted personnel. This will require continued development of cyberspace doctrine, tactics, techniques, and procedures, and continued integration into Army capstone documents. Cyberspace-related programs of instruction will be derived from joint institutional training programs and will be deconflicted, synchronized, and integrated to ensure use of Army training resources and Army-unique training requirements.

g. Future army concepts doctrine. The Army will integrate Army cyber requirements within the Army Concept Framework and identify what every leader, Soldier, and staff member should know about Army operations in the cyber domain, and determine how to integrate changes aligned to the joint cyberspace operations construct with Army requirements. FM 3-38 is the interim step to addressing this issue; however, broader doctrine that nests with emerging joint publications is required. Doctrine for Army integrated cyber operations is the next logical step for preparing and advising the Army on cyberspace operations at all echelons and joint integration. Under the proposed CEMA WfF construct, the Army will develop a functional concept for CEMA and integrate cyberspace operations within ADPs 3-0 and 5-0. An ADP and an ADRP for cyberspaces operations will describe how commanders, supported by their staffs, leverage the combined capabilities of the cyberspace operations combined arms team and achieve superiority in the cyberspace domain at the time and place of their choosing to help drive ULO outcomes.

h. WCCO. Leaders and Soldiers across all the WfFs will test in progressive levels of cyberspace operations skills at combat training centers, exercises, and home station training through force-on-force engagements in the cyberspace domain with highly skilled WCCO. The TRADOC G2 provides training and oversight to the WCCO to ensure cyber activities integrate within the WCCO IW plan, provides evaluation and feedback as part of the overall opposing force accreditation program, and is the source of WCCO doctrine. The development and employment of these specialized opposition forces will provide experience operating in a contested environment, enhancing Soldier readiness.

i. Live, virtual, constructive, and gaming. The Army will gain efficiencies and increase training effectiveness through live, virtual, constructive, and gaming training models supported with technology advances. Commanders will determine the proper mix within the integrated training environment to support mission command systems and the training audience effectively.

j. Experimentation, models and simulations. The Army does not have integrated and robust cyberspace experimentation through models, simulations or a battlelab collaborative simulation environment to develop, refine, and integrate cyber concepts and doctrine ideas with other CoEs and WfFs. The CEMA CoE will establish an organic battlelab collaborative simulation

environment hardware and software interface capability. Additionally, a joint and Army integrated cyberspace and cyber capability modeling and simulation effort can help avoid interoperability issues and eliminate duplication of effort. The endstate of this effort is an interoperable cyber community of practice and federation for collective experimentation and training capable of supporting TRADOC Campaign of Learning efforts, Army warfighter and tactical training exercises, and facilitate reachback problem solving for forces deployed forward.

k. Information warfare functional area. The Army should consider establishing an information warfare functional area to provision trained and ready cyberspace operations leaders. Technical expertise is largely resident in the Army signal, intelligence, EW, space, IO, and KM personnel management system; however, a new framework will elevate Army cyberspace operations practitioners to the next generation of leadership, bridging the land and cyber domains. This functional area will master the integration of multiple cyber-related disciplines and deliver strategic to tactical advantage across the human, cyberspace, and EMS battleground. An information warfare functional area will provide multi-disciplined Soldiers with career road maps for movement across the range of cyber mission areas. This will result in well-rounded, better-educated cyber leaders for the Army.

---

## **Glossary**

### **Section I Abbreviations**

ADP	Army doctrine publication
ADRP	Army doctrine research publication
AO	area of operations
AOR	area of responsibility
ARCIC	Army Capabilities Integration Center
ARCYBER	Army Cyber Command
ARSOF	Army special operations forces
ASCC	Army service component command
BCT	brigade combat team
CBA	capabilities based assessment
CEM	cyber electromagnetic
CEMA	cyber electromagnetic activities
CNA	capabilities needs analysis
CoE	center of excellence
COP	common operational picture
DA	Department of Army
DCO	defensive cyberspace operations
DINO	Department of Defense information networks operations
DODIN	Department of Defense information network
DOD	Department of Defense
DSCA	defense support of civil authorities
EMS	electromagnetic spectrum

EW	electronic warfare
EXORD	execute order
FM	field manual
GCC	geographic combatant commander
IC-ITE	intelligence community-information technology enterprise
ICT	information and communications technology
IE	information environment
IIA	inform and influence activities
IO	information operations
IT	information technology
JFHQ-C	Joint Force Headquarters (cyber)
JIE	joint information environment
JP	joint publication
KM	knowledge management
MI	military intelligence
NETOPS	network operations
NSA	National Security Agency
OCO	offensive cyberspace operations
OE	operational environment
OPE	operational preparation of the environment
Pam	pamphlet
RC	required capability
S&T	science and technology
SA	situational awareness
SIGINT	signal intelligence
SU	situational understanding
TIB	theater intelligence brigades
TRADOC	U.S. Army Training and Doctrine Command
ULO	unified land operations
U.S.	United States
USCYBERCOM	United States Cyber Command
WCCO	world-class cyber opposing force
WfF	warfighting function

## Section II

### Terms

#### **cloud computing**

A model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. (National Institute of Standards and Technology.)

#### **combat power**

The total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time.



**combined arms**

Synchronized and simultaneous application of the elements of combat power to achieve an effect greater than, if each element of combat power was used separately or sequentially.

**combined arms maneuver**

The application of the elements of combat power in unified action to defeat enemy ground forces; to seize, occupy, and defend land areas; and to achieve physical, temporal, and psychological advantages over the enemy to seize and exploit the initiative.

**content management**

Activity that focuses on managing digital and non-digital knowledge and information contained in any medium that conveys such content and provides awareness of relevant, accurate information through automated access to newly discovered or recurring information in a timely, efficient, and usable format.

**closed network**

A network designed not to be connected to the greater Internet and, therefore, inaccessible to the general public.

**cross-domain**

The combination of two or more of the military domains: ground, maritime, air, space, and cyberspace.

**cross-domain synergy**

The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others.

**cyber electromagnetic activities**

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

**cyberspace domain**

A global domain within the information environment consisting of the interdependent networks of information technology infrastructures, data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

**cyberspace operations**

The employment of cyberspace capabilities where the primary purpose is to achieve objectives in and through cyberspace.

**dark networks**

Networks connected to the greater Internet but hidden and inaccessible through normal means.

**defend**

The functions and tasks actively and passively performed to defend the LandWarNet from internal and external threats.

**defense support of civil authorities**

DOD support for domestic emergencies and for designated law enforcement and other activities.

**defensive cyberspace operations**

Passive and active operations to preserve the ability to utilize friendly cyberspace capabilities and protect networks and net-centric capabilities.

**DOD information network operations**

Actions taken to gain and maintain access to the cyber domain via the execution of architect, build, configure, secure, operate, maintain, and sustain functions in and through the LandWarNet.

**effect**

The physical or behavioral state of a system that results from an action, a set of actions or another effect; resulting outcome or consequence of an action; change to a condition, behavior, or degree of freedom (Joint Pub (JP) 1-02).

**electric fires**

The use of electromagnetic energy as either the primary source or the primary mechanism for destructive effects.

**electromagnetic spectrum**

The range of frequencies of electromagnetic radiation from zero to infinity divided into 26 alphabetically designated bands (JP 1-02).

**electromagnetic spectrum management**

Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures (JP 1-02).

**electromagnetic spectrum operations (joint)**

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 1-02).

**enterprise management**

The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security.

**exploit**

The penetration of enemy networks to gain intelligence or prepare targets for offensive operations.

**global commons**

The global commons consist of international waters and airspace, space, and cyberspace.

**human dimension**

That which encompasses the social, physical, and cognitive components of Soldier, civilian, leader, and organizational development and performance essential to raise, prepare, and employ the Army in unified land operations.

**homeland defense**

The protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President.

**information**

The meaning that a human assigns to facts, data, or instructions in any medium or form by means of the known conventions used in their representation.

**information assurance**

Action that protects and defends information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.

**information environment**

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

**information operations**

Integrated employment, during military operations, of information related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decisionmaking of adversaries and while protecting U.S. capabilities.

**Internet**

A means of connecting a computer to any other computer anywhere in the world via dedicated routers and servers.

**inform and influence activities**

The integration of designated information-related capabilities to synchronize themes, messages, and actions with operations to inform U.S. and global audiences, influence foreign audiences, and affect adversary and enemy decisionmaking.

**joint information environment**

A construct that facilitates the convergence of the DOD's multiple networks into one common and shared global network.

**key terrain**

Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant.

**knowledge creation**

Formation of new ideas through interactions between explicit and tacit knowledge in individual human minds.

**knowledge management**

Range of strategies and practices used in an organisation to identify, create, represent, distribute, and enable adoption of insights and experiences.

**knowledge operations**

Orchestrated activities that have defense objectives, focused on thoughts, thinking processes, and thought systems, and concerned with the ways and means by which meaning is assigned, derived, and shared.

**knowledge transfer**

Methodical replication and planned movement of expertise, wisdom, and tacit knowledge gleaned by Soldiers and leaders, transferred to subordinates and peers.

**LandCyber operations**

Activities that generate and exert combat power in and through cyberspace utilizing combined arms leaders, staffs, and formations to enable freedom of maneuver and action in land and cyberspace domains to deliver decisive effects.

**LandCyber maneuver**

Series of moves over cyber terrain to achieve a position of advantage over an adversary.

**LandWarNet**

The Army's contribution to the DODIN; consists of all globally interconnected, end-to-end sets of Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand.

**maneuver**

Employment of forces in the AO through movement in combination with fires to achieve a position of advantage in respect to the enemy.

**mission command**

The conduct of military operations through decentralized execution based on mission orders.

**network**

A single, secure, standards-based, versatile infrastructure linked by networked, redundant transport systems, sensors, warfighting and business applications, and services.

**network assurance**

Protection, detection, and proper response to any unauthorized activities against the DODIN.

**network operations**

DOD-wide operational, organizational, and technical capabilities for operating and defending the DODIN.

**offensive cyberspace operations**

Activities conducted to project power against adversaries in or through cyberspace.

**operational adaptability**

The ability to shape conditions and respond effectively to changing threats and situations with appropriate, flexible, and timely actions.

**operational preparation of the environment**

Non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations.

**partner**

Person, group, or nation working with the U.S. toward the achievement of one or more aims.

**signals intelligence**

Individual or combined communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted, and intelligence derived from communications, electronics, and foreign instrumentation signals.

**situational awareness**

The perception of environmental elements within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.

**space**

A medium like the land, sea, and air within which military activities are conducted to achieve U.S. national security objectives.

**stability operations**

Military missions, tasks, and activities conducted outside the U.S. in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.

**threat vector**

A specific computer-system vulnerability, along with the path and method in which it may be exploited.

**warfighting function**

A group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives.

**wide area security**

The application of the elements of combat power in unified action to protect populations, forces, infrastructure, and activities; to deny the enemy positions of advantage; and to consolidate gains in order to retain the initiative.

**Section III****Special terms****convergence**

Independent development of similar characteristics which lead to the merging of distinct technologies, industries, or devices into a unified LandCyber force.

**cyber**

Capabilities of computers, IT, networks, and virtual reality grouped to support capability analysis, strategy development, investment decisionmaking, capability portfolio management, and capabilities-based force development and operational planning.

**cyberspace (proposed)**

The applied combination of the naturally-occurring EMS and the man-made technical grid of networks and processors; overlaid by a virtual landscape on which information objects act as human surrogates to accomplish human ends.

**cyberspace control mission area**

Operations that provide freedom of maneuver and action in the cyberspace domain, enabled through the operation and defense of the Army network enterprise.

**cyberspace force enhancement mission area**

Operations that provide improved cyberspace and cross-domain SA facilitating knowledge operations.

**cyberspace support mission area**

Operations that enable end-to-end cyberspace functionality.

**cyberspace force application**

Operations that provide cyberspace exploit, attack, and influence capabilities to deliver effects in and through cyberspace.

**cyberspace SA**

Current and predictive knowledge of cyberspace and the OE upon which cyberspace operations depend.

**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.

**cyberspace terrain**

Physical and non-physical terrain created by and/or composed of the human layer, logical layer, and physical layer.

**hunting**

An internally-focused active defensive measure that detects advanced threats within friendly networks and take appropriate response actions.

**hunt teams**

Entities that actively search for and locate threats that have penetrated the Army enterprise, but not yet manifested their intended effects.

**NATIONAL  
SECURITY  
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, [nsarchiv@gwu.edu](mailto:nsarchiv@gwu.edu)