THE CYBER DOMAIN: A LEVIATHAN OR GIANT WAITING TO BE SLAIN WITH THE STONE OF DOCTRINE

A Monograph

by

MAJ Jason L. Glemser

United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2014-001

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
22-05-2014	SAMS Monograph	June 2013 - May 2014

4. TITLE AND SUBTITLE
The Cyber Domain: A Leviathan or Giant Waiting to Be Slain By the Stone of Doctrine

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Jason L. Glemser, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
250 Gibbon Ave
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
100 Stimson Ave.
Ft. Leavenworth, KS 66027-2301

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This monograph examines the Army's first doctrinal publication to address operations in the cyber domain, FM 3-38 Cyber Electromagnetic Activities (CEMA), to determine if it provides a doctrinal construct to meet emergent threats and rapid technology growth. Raising cyber to the domain level has created doctrinal implications for a domain that transcends and exists in the physical domains. Domain establishment indicates that dominance and superiority must occur, but dominance and superiority may be unachievable in the cyber domain. Understanding how cyberspace operations can occur simultaneously and concurrently in support of and independent of each other provides a new understanding of three tenets of Army operations: synchronization, integration, and depth. The complexity within the cyber domain has changed the understanding of the operational environment but provides opportunities to exploit vulnerabilities by fighting in and through the domain.

15. SUBJECT TERMS
Cyber Domain, Domain Definition, Theory and Doctrine Relationship, Cyber Electromagnetic Activities, Cyberspace Operations, Synchronization, Integration, Depth.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPONE NUMBER (*Include area code)*
(U)	(U)	(U)	(U)	60	

MONOGRAPH APPROVAL

Name of Candidate: MAJ Jason L. Glemser

Monograph Title: Cyber Doctrine: A Leviathan or Giant Waiting to be Slain with the Stone of Doctrine

Approved by:

_____, Monograph Director
Alice Butler-Smith, Ph.D.

_____, Seminar Leader
Michael R. Anderson, LTC, EN

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL, IN

Accepted this 22nd day of May 2014 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

ABSTRACT

THE CYBER DOMAIN: A LEVIATHAN OR GIANT WAITING TO BE SLAIN BY THE STONE OF DOCTRINE, by MAJ Jason L. Glemser, Army, 60 pages.

This monograph examines the Army's first doctrinal publication to address operations in the cyber domain, FM 3-38 Cyber Electromagnetic Activities (CEMA), to determine if it provides a doctrinal construct to meet emergent threats and rapid technology growth. Raising cyber to the domain level has created doctrinal implications for a domain that transcends and exists in the physical domains. Domain establishment indicates that dominance and superiority must occur, but dominance and superiority may be unachievable in the cyber domain. Cyber domain's youth lacks the influence of an accepted or tested military theory, however this has little impact on military operations since the cyber domain supports the US Army's theory and doctrinal construct of Unified Land Operations. The lack of a cyber theory does not diminish the importance and relationship between policy and strategy, but compresses the two through tactical actions in cyberspace operations which can provide strategic effects. Understanding how cyberspace operations can occur simultaneously and concurrently in support of and independent of each other provides a new understanding of three tenets of Army operations: synchronization, integration, and depth. The complexity within the cyber domain has changed the understanding of the operational environment but provides opportunities to exploit vulnerabilities by fighting in and through the domain. Innovative doctrine can provide the proper construct to exploit vulnerabilities and achieve desired effects within the cyber domain to enhance the Army's effectiveness in Unified Land Operations to achieve a position of relative advantage.

TABLE OF CONTENTS

ACRONYMS

ADP	Army Doctrine Publication
CEMA	Cyber Electromagnetic Activities
CO	Cyberspace Operations
DoD	Department of Defense
EMS	Electric Magnetic Spectrum
EW	Electronic Warfare
FM	Field Manual
JP	Joint Publication
SMO	Spectrum Management Operations
TRADOC	Training and Doctrine Command
US	United States
ULO	Unified Land Operations

ILLUSTRATIONS

Page

TABLES

Page

INTRODUCTION

> Like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, cyber. It trips off the tongue, and frankly I have found the concept liberating when I think about operationalizing this domain. But the other domains are natural, created by God, and this one is the creation of man. Man can actually change this geography, and anything that happens there actually creates a change in someone's physical space. Are these differences important enough for us to rethink our doctrine?[1]
>
> —General Michael V. Hayden, USAF, Retired
> "The Future of Things 'Cyber'"

Imagine a scenario in which a United States (US) Special Operations group combined with cyber specialists, plan to execute a raid into a hostile country to hack into the country's air defense network and disrupt or destroy the network, blinding the country just prior to a major invasion. Although not hard to imagine in the computer and information age of today, in 1990 this would have seemed preposterous. However, this plan was developed and proposed to the United States Central Commander, General Norman Schwarzkopf, prior to the start of the first Gulf War. The plan did not receive approval because of the risk and uncertainty of its success to cripple Iraq's air defense systems. Moreover, the wisdom of the time was that, if you wanted to destroy a country's air defense system, just bomb the systems components, which will provide a measurable means of effectiveness.[2]

---

[1]Gen Michael V. Hayden, "The Future of Things 'Cyber'," *Strategic Studies Quarterly* (Spring 2011): 4, http://www.chertoffgroup.com/pdf/The-Future-of-Things-Cyber-by-Michael-Hayden-Strategic-Studies-Quarterly-Spring-2011.pdf (accessed January 30, 2014).

[2]Richard A. Clarke and Robert K. Knake, *Cyber War: the Next Threat to National Security and What to Do About It* (New York: Ecco, 2012), 9. "Schwarzkopf thought the plan risky and unreliable. He had a low opinion of US Special Operations command and feared that the commandos would become the first Americans held as prisoners of war, even before the war started. Even worse, he feared the Iraqis would be able to turn their computers back on and would start shooting down some of the two thousand sorties of attacks he planned for the first day of the air war. "If you want to make sure their air defense radars and missiles don't work, blow them up first. That way they stay dead. Then go in and bomb your targets." Thus, most of the initial US and allied air sorties were not bombing raids on Baghdad headquarters or Iraqi Army divisions, they were on the air defense radar and missile sites."

The United States and the world have moved beyond the conventional understanding of only attacking targets using direct means of physical force. The rapid growth of computer networks and the internet has given rise to attacks occurring in cyberspace. To address the increasing concern of cyber-attacks and to combat threats in this newly contested domain, the US Department of Defense (DoD) added cyberspace as the fifth domain of war. In 2010 the DoD added cyberspace to the traditional four domains, land, air, maritime, and space and created a sub-unified command. All four services followed suite by creating a component specific cyber command. The rapid growth and uncertainty surrounding cyberspace and cyber-attacks has generated much needed discourse, as well as organization of military priorities to address the national and military vulnerabilities. However, the rapid expansion, growth, and emphasis on addressing cyber related vulnerabilities within the military, and specifically the Army, maybe causing a rush to address problems that are not necessarily the right ones that need to be solved.

Following the creation of the cyber domain as the fifth domain of war, the US Army created the Army Cyber Command in 2010. Since then, the Army has sought to define the problem of operating in this newly contested domain of war. In order to provide operating guidance, the US Army Combined Arms Center created the first dedicated field manual to address operations in cyberspace. Field Manual (FM) 3-38, *Cyber Electromagnetic Activities* (CEMA), was published in February 2014 to institutionalize the concept of CEMA and provide commanders and staffs guidance on conducting operations in the cyber domain. This monograph will argue that the current Army doctrinal construct for cyber operations is insufficient to meet emergent threats and constant rapid technology growth in cyberspace.

Three main reasons will be given to explain why the Army's field manual, which is dedicated to capturing how the Army views and conducts operations in cyberspace, is lacking as a doctrinal construct for operations in the cyber domain. The first reason is DoD's emphasis on categorizing cyber as a domain may focus on the wrong problem of domain relevance, instead of

the impacts of operationalizing cyberspace. The cyber domain cuts across all physical domains and is not restricted to geographical borders. Categorizing cyber as a domain may highlight the importance of cyberspace but may not capture the complexity of the entire system and systems that make up cyberspace. The second reason is the lack of a grand cyber theory can be problematic for doctrinal development. Additionally, technological advancements in cyberspace and the speed of advancements in technology pose problems for doctrinal development that has not previously existed in the traditional domains. The third reason is the Army's missed opportunity to effectively describe how three tenets of Army operations, synchronization, integration, and depth, are applied in cyberspace operations through time, space, and purpose.

United States cyber policy documents, scholarly publications to include cyber theorists, DoD and US Army doctrinal publications, and major military theories and theorists are surveyed in support of this monograph's thesis. An understanding of Unified Land Operations (ULO) as the US Army's theory of war and doctrinal capstone document shapes and influences how cyber doctrine integrates within Army operations. An analysis of the key institutional publications that led to the development of FM 3-38 provides a doctrinal framework reference.

The operational environment in which the Army operates has never remained static. The environment will continue to change and adapt to advancements in technology and social constructs. The cyber domain is the most recent development in warfare and, although it poses many challenges, each challenge creates opportunity.

WHAT IS THE CYBER DOMAIN?

This section explores the effects of raising cyber to the domain level, understanding military doctrinal, relevance of the domain connotation, and conceptual boundaries imposed by labeling the domain cyberspace. Cyberspace is only able to exist through its reliance on infrastructure but its effects go beyond the components that reside in the physical domains. The complexity of defining the cyber domain is compounded by its physical and informational

attributes, while the traditional physical domains are bounded by their physical characteristics. The span of influence of cyberspace goes beyond the traditional domain construct and understanding. Although cyber has already been deemed a domain, the impacts of making cyber a domain need to be understood. Simply calling the domain "cyberspace" links the domain to preconceived understandings or prejudices and constrains potential understanding of how cyberspace transcends and influences the other domains. A more comprehensive name may exist for the cyber domain that embodies the essence and relationships between the physical and cognitive realms.

In order to fully appreciate, and contribute to, cyber doctrinal developments it is important to understand the significance of elevating cyber to the domain level. The US 2011 *Department of Defense Strategy for Operating in Cyberspace* developed five strategic initiatives to provide a comprehensive approach to defend United States interests in cyberspace. The DoD's first strategic initiative directed the treatment of cyberspace as an "operational domain to organize, train, and equip so DOD can take full advantage of cyberspace's potential."[3] While the elevation of cyber to a domain was perhaps the most significant recognition of the compounding nature of threats in cyberspace, it may have unintentionally forced the discussion away from the properties of cyberspace and its impacts on modern warfare.

Although, the DoD recognized the prominence of cyber issues, raising cyberspace to a domain may have complicated the issue by fixing a problem before the root cause of the problem was identified or fully understood. In his essay, "Cyberspace Is Not a Warfighting Domain," Martin C. Libicki's argues that, whether cyberspace is a domain or not is not the issue. Rather the effort to make cyber the fifth domain misrepresents the problem; which is really, "what can and

[3]Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 3.

should be done to defend and attack networked systems."[4] The miss identification of the problem has led to "strategists and operators to presumptions or conclusions that are not derived from observation and experiences."[5] Not properly framing the problem in regards to cyberspace issues has led to an outcome that centers on "connotations rather than denotations as the problems."[6] If the problem has not been correctly defined then the significance or essential properties may not be understood and the decision to make cyber a domain may solve a problem but not necessarily the right problem.[7]

Libicki explains that, even though the domain is man-made, it is cyber's malleability that makes it different. The design of the internet, computers, and software are subject to alteration or control by someone other than their creators because of the relationship that each element plays in the makeup of the complex system of cyberspace. In order for the system of cyberspace to function, each component is designed to communicate through relationships in the physical domains. Even Wi-Fi communication is bound through components of input and reception moved through the electric magnetic spectrum (EMS) that naturally exists in the space domain. The inherent relationship design of the physical components of cyberspace creates vulnerability through the nature of the open system which exists in cyberspace.[8] Even if a country or military

---

[4]Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 322, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf (accessed January 30, 2014).

[5]Ibid.

[6]Ibid.

[7]Jamshid Gharajedaghi, Systems *Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*, 2nd ed. (Boston, MA: Butterworth-Heinemann, 2006), 126. "We fail more often not because we fail to solve the problems we face, but because we fail to face the right problem. We have been taught how to solve problems, but never how to define one?"

[8]Neil E. Harrison, ed., *Complexity in World Politics: Concepts and Methods of a New Paradigm*, Suny Series in Global Politics (Albany: State University of New York Press, 2006), 8. Harrison describes social systems as open systems. "Open systems are susceptible to external influences and internal,

has the ability to design its own system, at some point a transfer of data or information occurs, opening the system to the potential of being altered in a manner or form other than its designed purpose.

Conceivably one of the greatest hazards in making cyber a domain is the institutional implications of domain dominance that exists in the military. By making cyber a domain, it unintentionally brings the "notion of domain superiority-the notion that power in a domain can prevent adversaries from doing anything useful in it."[9] Even though no one US military service is officially responsible for defending or conducting operations specifically in a domain, the natural structure of the US military eludes proponency. The nature of the military's organization has led to proponents of each specific domain, due to the emphasis of the specific service. The Army generates land power, which conducts operations in the land domain. The Air Force generates air power that specifically focuses on operations in the air and space domains. The Navy generates naval power that focuses on the maritime domain. All three service's force structures are built to facilitate operations in the physical domain that they are aligned against.

Each of the US military services has developed their respective capstone doctrine that revolves around the domain in which they predominately operate. All of the service's doctrine builds upon dominance and superiority, which is very applicable to traditional warfare, but may not be achievable in the cyber domain. The first of the US Army's two capstone documents, Army Doctrine Publication (ADP) 1, *The Army*, states that it provides the nations land power and that Americans expect it to dominate and win decisively.[10] In the joint context, one critical capability that land power provides is to "secure and support bases from which joint forces can

---

qualitative change and emergence and outcomes might be the result of many different causes and the same cause might lead to different outcomes."

[9]Libicki, "Cyberspace Is Not a Warfighting Domain," 332.

[10]Department of the Army, Army Doctrine Publication 1-0, *The Army* (Washington, DC: Headquarters Department of the Army, 7 November 2012), 1-7.

influence and dominate the air, land, and maritime domains of an operational environment."[11] The US Army's Cyber Command describes dominance as an integral part of its mission in the cyber fight and it must dominate the information environment.[12] The US Air Force's capstone doctrine states that airpower seeks to "dominate the fourth dimension."[13] The Navy capstone doctrine seeks to provide naval forces that "dominate the operational environment from which we project power at sea and ashore."[14] Dominance is an ingrained military institutional norm that may cloud realities in the cyber domain.

In the application of traditional military capabilities and force, the ability to dominate in the land, air, and maritime domains is ingrained in the rationality of military power. The ability to dominate in the four physical domains creates the notion of superiority. If superiority is achieved then who ever maintains superiority is able to keep the other belligerent from conducting meaningful operations in that domain. However, cyberspace is not unitary, its very composition consists of more than two belligerent sides, and everyone else still exists in cyberspace.[15]

While it may not be possible to dominate the entire cyber domain it may be possible to dominate an effect associated with cyber. In 2008, Russia kept Georgia's state leaders from communicating effectively with the Georgian population.[16] While Russia was able to dominate a

---

[11]Ibid., 1-4.

[12]US Army Cyber Command, "Army Cyber "Command; Army Cyber," http://www.arcyber.army.mil/org-arcyber.html (accessed March 19, 2014). Network dominance is an integral part of the cyber fight–today and tomorrow. Cyber threats demand new approaches to managing information, securing information, and ensuring our ability to operate. Cyberspace is on par with the other war-fighting domains of land, sea, air and space. It is in cyberspace that we must use our strategic vision to dominate the information environment throughout interdependencies and independent systems.

[13]US Air Force, Air Force Doctrine Document 1, *Air Force Basic Doctrine, Organization, and Command* (Maxwell AFB, AL: United States Air Force, 14 October 2011), 19.

[14]Naval Service, Naval Doctrinal Publication 1, *Naval Warfare* (United States Navy, 1 March 2010), 45.

[15]Libicki, "Cyberspace Is Not a Warfighting Domain," 332.

[16]Ibid., 327.

portion of message control, it did not dominate the internet. Russia used cyberspace not as a weapon but as a means of delivering a weapon of information control. However, due to the internet's susceptibility to alteration by outside parties Georgia was able to contract US companies to redo its network structure to regain control of their systems.[17] The internet, which exists in cyberspace, contributes an inherently social aspect through social media that facilitates a constant struggle in controlling its main product, information. The perception of dominance and control in cyberspace is misleading. The danger of assuming dominance creates a false perception of security that leads to vulnerabilities. No matter how closed a network seems the assumption should always be that the system are breached or are being probed to be breached. An assumption of a secure network provides a false sense of security and may preclude network administrators from detecting minor variations in the system.

Although the argument may be moot if cyber is a domain, an understanding of the impact is not. Cyberspace's unique characteristics set it apart from the geographical boundaries of the physical domains. Even though cyberspace has components that exist in the physical domains its effects are achieved through its cognitive traits. The uniqueness of the cyber domain will force a change in institutional perception, away from the traditional understanding of dominance and domain superiority. In order to understand the domain, the domain must be defined. Defining the domain is important in order to understanding doctrinal definitions and significance of the domain construct.

Defining the Cyber Domain

Elevating cyber to domain status produced the necessity for an established definition in order for the DoD to create a shared understanding of the domain. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines cyberspace as: "A

[17]Ibid.

global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[18] JP 1-02 does not define the term cyber domain like it defines the air domain or maritime domain, but rather defines cyberspace within a larger context of a global domain. The term cyberspace was around long before cyber became a domain, so by using the word cyberspace to define the domain may be adding to the confusion of how to define this new domain.[19]

Joint Publication 1-02 has specific definitions that correspond to the terms air domain and maritime domains. Interestingly, the land domain is not defined in JP 1-02, but a definition is found in Army Doctrine Reference Publication 1-02, *Operational Terms and Military Symbols*. However, all three domains are organized in an adjective noun relationship and described by their physical geographical traits.[20] For instance, the air domain starts at the earth's surface and extends to where the atmosphere becomes negligible.[21] The maritime domain consists of oceans, bays, costal area, and the airspace above these.[22] The land domain is anything on the earth's surface or close to the surface.[23] All three are easy to comprehend through their distinguishable geographical qualities. Cyberspace is different from the traditional domain construct and consists of a global

---

[18]Joint Chiefs of Staff, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Joint Chiefs of Staff, 15 September 2013), 68.

[19]William Gibson is credited with creating the term "cyberspace" in his 1984 science fiction book *Neuromancer*.

[20]Land domain—is part of the traditional physical domains (air, sea, and space) and includes those mission areas on the land surface or close to the surface, Department of the Army, Army Doctrine Reference Publication 1-02, 3-1. Air domain—the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible, Joint Chiefs of Staff, Joint Publication 1-02, 7. Maritime domain—the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals, Joint Chiefs of Staff, Joint Publication 1-02, 164.

[21]Joint Chiefs of Staff, Joint Publication 1-02, 7.

[22]Ibid.

[23]Department of the Army, Army Doctrine Publication 1-02, 3-1.

domain within the information environment, dependent on the infrastructure that exists in the physical domain, which enables it to exist.[24] Cyberspace's definition drastically differs from the definitional description of the land, air, and maritime domains geographical traits and transcends to an environment that exists globally, beyond physical components which consist of data.

The youngest domain prior to cyberspace, the space domain, provides contextual similarity between the cyber domain and space domain in regards to the description of an environment. JP 1-02 does not define the space domain; it defines the space environment. The space environment is "the environment corresponding to the space domain, where electromagnetic radiation, charged particles, and electric and magnetic fields are the dominant physical influences, and that encompasses the earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere."[25] Like cyberspace, the definition of the space environment uses the word environment to conform to the domain of space.

The two youngest domains are not defined in the military's dictionary as pure domains but as environments within a larger context. Meaning that land, air, and maritime domains are self-constrained by geography, limiting them to a specific region. While cyberspace and space exist in environments that surround all objects not constrained to or by a specific region. People conduct activities on or in land, air, and maritime domains but are surrounded by the environments of cyberspace and space domains, from which those activities are being conducted. Unlike land, air, and maritime domains, space and cyber begin to move the paradigm of boundaries away from physical features to an environmental framework from which they operate in, thus creating a more complex system that may not be as easily defined through traditional doctrinal means.

---

[24]Joint Chiefs of Staff, Joint Publication 1-02, 68.

[25]Ibid., 255.

If domain distinction is deemed important, then it would seem logical to have domain defined in military doctrine. However, there is no definition for domain in JP 1-02. Since there is no Joint or Army definition of domain, a review of the definition of a domain is required. Merriam-Webster lists 10 definitions of domain. Of those 10; six have applicability to defining domain in the cyber construct. Three of those six center on complete and absolute ownership of land. One defines it as a region marked by some physical feature, one as a sphere of knowledge, influence, or activity, and the last defines it as a subdivision of the internet consisting of computers or sites usually with a common purpose and denoted in internet addresses; a domain name.[26]

Recognizing that domain is undefined in joint doctrine, Dr. Patrick D. Allen and Dennis P. Gilbert developed six key features of a domain in their monograph "The Information Sphere Domain Increasing Understanding and Cooperation."[27] The six key features of a domain were developed in order to quantify the current physical domains and set criteria to judge the creation of a new domain, since joint military doctrine did not define domain. Allen and Gilbert determined that in order to be considered a domain the domain must require unique capabilities, it is not included in another domain, both friendly and enemy share a presence in that domain, control of the domain can occur, opportunity exists for interaction with other domains, and the domain creates opportunity for asymmetric advantage.[28] These six features provide a base to

---

[26]*Merriam-Webster*, s.v. "Domain," http://www.merriam-webster.com/dictionary/domain?ref=office (accessed March 25, 2014).

[27]Dr. Patrick D. Allen is a systems engineer from Johns Hopkins University Applied Physics Lab Information Sciences Division and retired US Army Reserves Colonel. Dennis P. Gilbert is currently serving as the Special Assistant and Cybersecurity Strategic Advisor in the Office of the deputy Chief Information Officer for Cybersecurity, and retired US Air Force Officer.

[28]Christian Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Perspectives On Cyber Warfare*, vol. 3 of *Cryptology and Information Security Series* (The Netherlands: Ios Press, 2009), 134. Those six features are: "1) Unique capabilities are required to operate in that domain, 2) A domain is not fully encompassed by any other domain, 3) A shared presence of friendly and opposing capabilities is

build upon the understanding of any domain and further enhance the Merriam-Webster's definition.

According to Allen and Gilbert, all four of the physical domains meet these requirements. For instance, to operate in the air domain aircraft are required, it is distinguishable from the other domains, it can be opposed by enemy aircraft or air defense systems, presence creates the need to exert some type of control, operations are linked to other capabilities and objectives, and through operating in it, opportunities are created to gain an asymmetric advantage.[29]

In order to develop a distinct definition of domain, Allen and Gilbert focus on Merriam-Webster's Dictionary definition of domain and its description as "a sphere of activity, interest, or function."[30] Attention is drawn to the definition of sphere, which is defined by Merriam-Webster as an "area or range over or within which someone or something acts, exists, or has influence or significance, such as a public sphere."[31] The definition of a sphere denotes that it not only includes physical environments, but also non-physical environments as well.[32]

To encompass both physical and non-physical environments Allen and Gilbert propose the definition of a domain as; "the sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects."[33] Using the stated definition of a domain, Allen and Gilbert argue that the DoD's definition of cyberspace in JP 1-02 is a good definition for cyberspace but

---

possible in the domain, 4) Control can be exerted over the domain, 5) A domain provides the opportunity for synergy with other domains, and 6) A domain provides the opportunity for asymmetric across domain."

[29]Czosseck and Geers, 134-135.

[30]Ibid., 132.

[31]*Merriam-Webster*, s.v. "Sphere," http://www.merriam-webster.com/dictionary/domain?ref=office (accessed March 25, 2014).

[32]Czosseck and Geers, 132.

[33]Ibid.

an inadequate definition for the cyber domain. Allen and Gilbert pose replacing the cyber domain name with the term "information sphere" to serve as the overarching domain that captures the relationships that exist between the cognitive, information, and cyber domains.

The reason for this paradigm shift in naming is that, just as the maritime domain consists of both surface and subsurface actions, it consists of two parts that make up the whole of the domain. As such, cyberspace is only one component that makes up the larger information sphere.[34] The information sphere would be defined as, "The space of relationships among actors, information, and information systems that form a sphere of interest and influence in or through which information-related activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects."[35]

The definition of information sphere highlights that the three major components (actors, information, and the information systems) must reside in one of the physical domains. In order for the information to get into the information sphere, there must be entry and exist points that link it to the other domains but those entry and exit points do not fully capture the entire information sphere from the linked domain.[36] The relationships between the existing physical domains and the information sphere domain are demonstrated in the figure 1.

---

[34]Czosseck and Geers, 136. We believe that this is a good definition of cyberspace, but believe that cyberspace is still a subset of the larger Information Sphere domain. Just as naval surface actions and submarine actions are two components of the Sea domain, cyberspace, cognitive, and information are components of the more encompassing Information Sphere.

[35]Czosseck and Geers, 136.

[36]Ibid., 138.

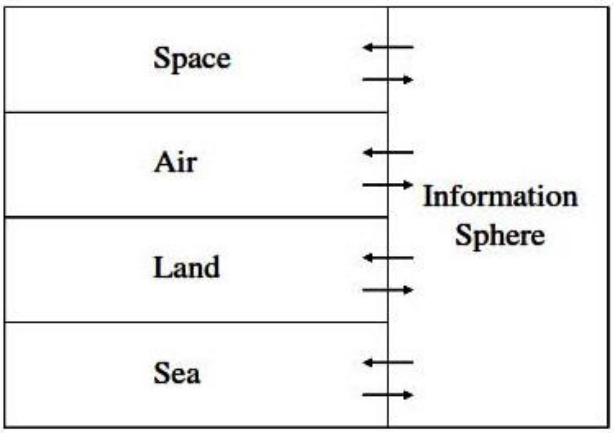

Figure 1. Information Sphere

Source: Christian Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Perspectives On Cyber Warfare*, vol. 3 of *Cryptology and Information Security Series* (The Netherlands: Ios Press, 2009), 138.

The proposal of creating the information sphere to replace the construct of the current cyber domain is interesting, because it does not strictly focus on the means but rather the relationships that exist between the components that make up the information sphere. This lends to the perceived function of cyberspace; is cyberspace itself the weapon or merely the means to deliver a weapon through a desired effect? While Allen and Gilbert believe that the ability to exert control is necessary as a key function of a domain, the ability to control such a complex environment may prove to be an unrealistic goal.

While it may be impossible to exert control across the entire information sphere, the entry and exit points (figure 1) provide potential critical vulnerabilities that may be exploited to exert some type of control for specific effects in time and place. The entry and exist points resemble movement corridors and provide likely places to exploit. A more feasible application of control in accordance with the Army's tactical task of control would be to focus at specific temporal and

spatial points of transfer between domains. This would focus on the application of control instead of trying to control an entire domain.[37]

However, the doctrinal definition shift comes from moving away from the physical influence of control to the temporal and spatial aspects that exist in cyberspace. The end result is that conditions are created which prevent the enemy from using a virtual place and which will facilitate the accomplishment of friendly operations. This example of the use of the word control highlights that both doctrinal definitions and the conceptual understanding of cyberspace may need to change. By synthesizing current doctrinal definitions, and the relationships among actors, information, and infrastructure that enable the transfer of information lends credence to the need to better define the cyber domain. The information sphere provides a good example of how to encompass the essence and reality of the complexity that exists when referring to cyberspace. By accurately understanding the 21st century's informational environment, the construct of the information sphere does not solely look at one aspect of cyberspace but tries to focus on the entire system as a whole and the sub systems that make up the larger system. The information sphere paradigm may help commanders better conceptualize their operating environment and provide the construct to make decisions based on "conditions, circumstances, and influences that affect the employment of capabilities."[38]

The debate of making cyber a domain may seem futile, but it does have implications for doctrinal development. As a domain, it would seem appropriate to rely on a theory to drive doctrinal development. The physical domains have had many specific theories throughout their

---

[37]Department of the Army, Army Doctrine Reference Publication 1-02, 1-10. Control—A tactical mission task that requires the commander to maintain physical influence over a specified area to prevent its use by an enemy or to create conditions necessary for successful friendly operations.

[38]Joint Chiefs of Staff, Joint Publication 1-02, 102. Operational environment—A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Also called OE.

history to shape, influence, and evolve their domain. As a newly created domain, cyberspace does not have a grand strategist to draw upon. The domain will be defined by current perception and understanding, which will require theoretical thinking that, is grounded in human affairs and the comprehension of the order of cyberspace.[39] The importance of doctrine to guide this domain cannot be overlooked, since JP 1-02 describes doctrine as the "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application."[40]

The challenges that exist in creating or labeling the cyber domain are only compounded by the necessity to create cyberspace doctrine. The rapid growth of the cyber domain and the constant advancements in technology will pose additional challenges to doctrinal developments. Coupled with the lack of theorist consensuses, cyber doctrine writers will need to hold true to the idea that, doctrine must serve as a guide and not act as a set of fixed rules in an environment that is constantly growing and changing.[41]

TECHNOLOGY, THEORY, AND DOCTRINE

This section focuses on the impact of technology on doctrine and how the rate of technological advancements in cyberspace, creates challenges in maintaining relevant doctrine that is not outpaced by advancements in technology. The link between theory and doctrine points to the important relationship that is shared between both, to include the progression of what led to the development of the Army's cyberspace field manual, FM 3-38, *Cyber Electromagnetic Activities*. Although there is no grand theorist guiding the development of the cyberspace theory,

---

[39]James N. Rosenau, "Thinking Theory Thoroughly," in *The Scientific Study of Foreign Policy*, ed. James N. Rosenau (London: Frances Pinter, 1980), 32.

[40]Joint Chiefs of Staff, Joint Publication 1-02, 86.

[41]Department of the Army, Army Doctrine Publication 3-0, *Unified Land Operations* (Washington, DC: Department of Defense, 10 October 2011), 1.

the Army's operating concept of ULO serves as the service's overarching theory that any cyber specific doctrine must support.

The rate of technological advancement poses new challenges to the development and maintenance of relevant doctrine to address rapid changes in technology. At first glance, the relationship between technological growth and military doctrine may seem irrelevant, since doctrine tends to guide implementation. However, the military's dependence on technology creates a relationship that influences the rate of employment in the cyber domain. In 2003 *The National Strategy to Secure Cyberspace* was the first national level strategy that acknowledged, "cyberspace is the nervous system-the control of our country."[42] The 2003 strategy sought to develop a broad strategy that could leverage the whole of government, to include state and local, private business sector, and the American people. Acknowledgement of the role that the private sector has in developing technology, that private citizens and the government have become reliant on, underscores the interdependence that exists between business and government. In order to develop significant doctrine, the civilian military relationship in the cyber domain needs to be exploited to maximize the technological aspect of cyberspace.

In 1971, the Intel Corporation introduced the world's first microprocessor.[43] One of Intel's co-founders, Gordon Moore, developed Moore's Law, which states that the industry's technology will be able to improve circuits at a rate of every two years, doubling the number of micro-components of each chip.[44] While the rate of improvement has seen some plateaus, generally the sustained rate of improvement has been at one to two years, and some predict the

---

[42]The President of the United States, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), vii.

[43]Intel Company, "Intel Facts," http://www.intel.com/content/www/us/en/company-overview/company-facts.html (accessed March 17, 2014).

[44]Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, DC: Center for Technology and National Security Policy, 2009), 149.

industry growth rate will be able to be maintained past 2020. Recognizing the growth in technology, the only way for the military to quickly implement the updates, was to grow dependent on commercial off-the-shelf technology.[45]

Individual components of computers and networks are improving at a substantial rate. Networks that enable the connectivity to communicate share a law similar in scope to Moore's Law, known as Metcalfe's Law. Robert Metcalfe, one of the inventors of Ethernet technology, stated, "the value of telecommunications network is proportional to the square of the number of its users."[46] Metcalfe's premise is that the value of networks to the community not only grows linearly but is multiplied by the number of users itself.[47] The rate at which change is occurring in the systems that make up the environment of the cyber domain, is occurring at a rate that will challenge military doctrine to maintain pace, since the application of implementation is so heavily reliant on technology.

While the physical domains do not change over time the cyber domain is changing constantly. The physical principles that govern the land, air, maritime, and space domain have not changed. However, cyberspace is changing at a rate that may challenge any specific theory. Technological implementation interfaces with the social and cognitive nature of the environment, which composes the three layers of cyberspace: physical, logical, and cyber persona.[48] The constant changes and development in the cyber domain will drive a close civilian-military relationship, to develop doctrine to guide implementation and specific tactics and techniques to conduct operations.

---

[45]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, *The United States Army's Cyberspace Concept Operations Capability Plan 2016-2028* (Fort Monroe, VA: Department of the Army Headquarters, United States Army Training and Doctrine Command, 22 February 2010), 12.

[46]Kramer, Starr, and Wentz, 149.

[47]Ibid.

[48]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, 8.

Cyber domain's structural components exist in the logical layer that comprise cyberspace. The component parts that make up cyberspace are tied to physical locations comprised of multiple parts and circuits that have great structural complexity; it is known and understood how components will work together.[49] The social layer within the cyber domain is characterized by interactive complexity, since it consists of the users of the system which provides the human aspect that is non-linear and which the "link between cause and effect is ambiguous."[50] The three layers of cyberspace combine the predictability of structural complexity and the unpredictability of interactive complexity creating a complex adaptive system that is "learning and adapting adding a temporal dimension to complexity" in the cyber domain.[51]

The ability to understand how the domain is structured in both the physical realm and in its cognitive realm will facilitate better environmental understanding and doctrinal development. Although the pace of change in technology is a constant and shows no signs of slowing down, close civilian-military relationships will maximize integration of technology and doctrine. The understanding of some of the driving laws, such as the Moore and Metcalfe Laws, provides an understanding of components that make up the system and assist in the military understanding of variables that drive the operational environment, whether in the cyber domain or physical domains.

Theory and Doctrine Relationship

In his famous book *On War*, Carl Von Clausewitz states that,

> [T]heory should cast a steady light on all phenomena so that we can more easily recognize and eliminate the weeds that always spring from ignorance; it should show

[49]US Army Training and Doctrine Command, TRADOC Pamphlet 525-5-500, *The United States Army Commander's Appreciation and Campaign Design Version 1.0*. (Fort Monroe, VA: Department of the Army, 28 January 2008), 6.

[50]Ibid.

[51]Ibid.

> how one thing is related to another, and keep the important and the unimportant separated. If concepts combine of their own accord to form that nucleus of truth we call a principle, if they spontaneously compose a pattern that becomes a rule, it is the task of the theorist to make this clear.[52]

Military theory continues to evolve to provide that steady light, which Clausewitz refers to, but where concepts combined and created principles, those truths are now conceptualized in doctrinal principles. A dependency between theory and doctrine has emerged. Even though doctrine and theory have both existed independent of one another, it has been the interplay between the two that has captured the full benefits of implementation.

Political policy also plays a fundamental role and influence in the development of theory and doctrine. Policy shapes and guides strategy to achieve political objectives. The interplay between theory and doctrine influenced by policy, through implementation of strategy, is exemplified by Clausewitz's famous quote, "War is merely the continuation of policy by other means."[53] Although the quote has been used in multiple writings in varying context, it is even more applicable to the development of cyber doctrine. The sheer youth of the cyber domain, coupled with the recognition of national dependency, exemplifies the need to develop the guiding light of doctrine.

Moving past the stated argument of creating the cyber domain and the chosen name of cyberspace as the domain name, the impacts of domain creation are explored among policy, theory, and doctrine. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Network World* and the *Department of Defense Strategy for Operating in Cyberspace* provide the nation's cyber specific strategy for operating in cyberspace. Since policy becomes strategy

---

[52]Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret, Indexed ed., repr. ed. (Princeton, NJ: Princeton University Press, 1989), 578.

[53]Clausewitz, 87. War is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means. The political object is the goal, war is the means of reaching it, and means can never be considered in isolation from their purpose.

upon implementation, strategy should be influenced by theory, in order to bridge the gap between policy and doctrine which enforces that strategy. J.C. Wylie captures this relationship in his book *Military Strategy.* Wylie describes theory as the tool that links ideas and experiences adapted to apply in reality.[54] Theory then influences the development of doctrine, since doctrine is the instrument used to achieve the desired results of the theory applied.

Wylie describes four general theory categories that basically correspond to land, air, and maritime domains. Those theories are "continental, the maritime, and the air theories, and the Mao theory of the 'wars of national liberation.'"[55] Regardless of whom Wylie attributes each theory to; he is indirectly associating each theory to a domain. Since cyberspace has achieved domain status, it should have an acceptable theory, as the other domains. The lack of cyber theory should not be alarming though. Historically, technology has always been employed in warfare prior to the emergence of a theory or doctrine.

Understanding the impacts of fighting in a new domain are captured by what David Aucsmith calls "war from the domain and war within the domain." Aucsmith, the Senior Director at Microsoft Institute for Advanced Technology in Governments, argues that in "the natural development of a domain of war, the capabilities of the new domain are first used to project power from the new domain onto another domain."[56] Aucsmith uses the example of the introduction of aircraft in World War I. Aircraft initially conducted reconnaissance and observed from the air and evolved into attacks from the air onto ground forces. This led to the development

---

[54]J. C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, NJ: Rutgers University Press, 1967), 35. "The theory serves a useful purpose to the extent that it can collect men, sort out which of them may have a valid transfer value to a new and different situation, and help the practitioner to enlarge his vision in an orderly, manageable and useful fashion-and then apply it to the reality with which he is faced."

[55]Wylie, 37.

[56]David Aucsmith, "A Theory of War in the Cyber Domain," March 5, 2012, 5, https://www.academia.edu/1753317/A_Theory_of_War_in_the_Cyber_Domain_An_Historical_Perspective (accessed December 26, 2013).

of aircraft with the specific task to fight within the air (domain), in order to prevent the effects on the ground or land forces. The progression begins; the transition of fighting, to fighting within a domain, as technology and strategies progress or catch up.

The lack of cyber theory may not be an issue since theories only stand for as long as they are proven or disproven. Current military doctrine has evolved to encompass multiple theories that have survived the test of battle, along with experiences and lessons learned from those previous conflicts. The US military draws from across all the classical and prevailing theories of war to support the joint concept of Unified Action, which seeks to synchronize a whole of government approach to include all government and non-government agencies, Multinational partners, and private sector organizations.[57] Martin C. Libicki explains in his article, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," that even the beloved Clausewitz's book *On War* was not an instant classic.[58] Clausewitz's influence in Germany was gradual; a generation removed from him, and did not become widely known in the United States until after 1945.[59] Theorists often overstate the importance of their theory when advancing their cause. Libicki explains that if a cyber-theorist would emerge he would most likely sound the same common alarms that most previous theorists have used:

> 1) cyber war is totally important,
> 2) those who wield its power should fight to win wars on their own rather than helping warriors in other domains, and

---

[57]Joint Chiefs of Staff, Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: Joint Chiefs of Staff, 25 March 2013), II-7. Unified action synchronizes, coordinates, and/or integrates joint, single-Service, and multinational operations with the operations of other USG departments and agencies, Non-Governmental Organizations, International Governmental Organizations (e.g., the United Nations [UN]), and the private sector to achieve unity of effort (see Figure II-2). Unity of command within the military instrument of national power supports the national strategic direction through close coordination with the other instruments of national power.

[58]Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 24.

[59]Ibid.

3) war fighters in those other domains should take their strategic cues from what takes place in cyberspace.[60]

Perhaps it should not be lost that the land domain is where all inhabitants live and must begin before entering any other domain. Sir Julian Corbett captured this idea best in *Some Principles of Maritime Strategy.* "Since men live upon the land and not upon the sea, great issues between nations at war have always been decided–except in the rarest cases–either by what your army can do against your enemy's territory and national life or else by the fear of what the fleet makes it possible for your army to do."[61] Although there is no grand strategist to drawn upon in developing cyber domain theory at this moment, DoD has its theory of Unified Action from which each service has developed support theories and doctrine to support the joint forces. In the absence of a grand strategist in cyber theory, it would seem the most appropriate step would be to integrate cyberspace into existing doctrine.

Unified Land Operations: the United States Army's Theory of War

A cyber domain's uniqueness is that it transcends all domains and, the fact that it was created, may add to the difficulty in its application and in the execution of military operations. Jeffery Carr in his book, *Inside Cyber Warfare*, states that, "Cyberspace as a warfighting domain is a very challenging concept. The temptation to classify it as just another domain, like air, land, sea, and space is frequently the first mistake that's made by our military and political leaders and policy makers."[62] Although the Army did not declare cyber a domain, it must respond to the addition of the cyber domain and prepare the force.

---

[60]Ibid., 34.

[61]Sir Julian Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: United States Naval Institute, 1988).

[62]Jeffrey Carr, *Inside Cyber Warfare*, 2nd ed. (Beijing: O'Reilly Media, 2012), xiii.

The US Army's way of conducting and executing operations has come to incorporate numerous aspects from military theorists, along with incorporating many lessons learned from previous conflicts. The purpose here is not to show the development of US Army theory and doctrine through a historical lens, but to state that ULO is the Army's theory for how it conducts war. ADP 3-0, is the publication that encompasses Unified Land Operations. ADP 3-0 is unique in its characteristics, since it combines the aspects of theory and doctrine in one overarching manual that describes predominant principles and teaches how the Army employs forces, combining the science and art of operations. This combination corresponds with Clausewitz's purpose for theory: "the function of theory is to put all this in systematic order, clearly and comprehensively, and to trace each action to an adequate, compelling cause."[63] Not only does ULO put the Army's overarching theory and doctrinal principles in systematic order, it also supports the joint doctrine's concept of Unified Action.

Army Doctrine Publication 3-0 is the Army's second of two capstone manuals, "ADP 3-0 presents overarching doctrinal guidance and direction for conducting operations. It constitutes the Army's view of how it conducts prompt and sustained operations on land and sets the foundation for developing the other principles, tactics, techniques, and procedures detailed in subordinate doctrine publications."[64] ADP 3-0 is the Army's "central idea"; it provides the bases for all other Army doctrine, training, and professional development. As such, ADP 3-0 meets five key areas that Dr. Stuart H. Starr states should be present for any theory of warfare.

> First, it should introduce and define key terms that provide the foundation of the theory. Second, it should give structure to the discussion by categorizing the key elements of the theory. Third, it should explain the elements in these categories by summarizing relevant events and introducing key frameworks or models. Fourth, it should connect the various

[63]Clausewitz, 578.

[64]Department of the Army, Army Doctrine Publication 3-0, ii.

> elements of the subject so that key issues are treated comprehensively. Finally, it should seek to anticipate key trends and activities sot that policy can be germane and useful.[65]

Unified Land Operations meets Starr's five criteria as stated in ADP 3-0's preface; "presents overarching doctrinal guidance and direction for conducting operations. It constitutes the Army's view of how it conducts prompt and sustained operations on land and sets the foundation for developing the other principles, tactics, techniques, and procedures detailed in subordinate doctrine publications."[66] By describing the predominant principles of Army operations, it lays the foundation for how it will capture its core "institutional belief system."[67] Capturing the Army's institutional belief system in its capstone doctrine is important because it determines how it fights, its relationship internally and externally, and the institutional culture that it desires.[68]

Dr. Aaron P. Jackson, in his monograph "The Roots of Military Doctrine: Change and Continuity in Understand the Practice of Warfare," describes doctrine as a belief system. This "belief system regards accepted paradigms by which a military understands, prepares for, and (at least in theory) conducts warfare."[69] Jackson's definition of doctrine as a belief system, accurately describes the Army's two-paragraph definition of doctrine that describes it as a "body of thought."[70] The linkage between theory and doctrine can continue through examination of Jackson's linage of epistemology to doctrine carried through to theory.

---

[65]Czosseck and Geers, 19.

[66]Department of the Army, Army Doctrine Publication 3-0, ii.

[67]Dr. Aaron P. Jackson, *The Roots of Military Doctrine: Change and Continuity in Understanding the Practice of Warfare* (Fort Leavenworth, KS: Combat Studies Institute Press, 2013), 1.

[68]Ibid.

[69]Ibid., 6.

[70]Department of the Army, Army Doctrine Publication 3-0, 1, 2.

Jackson explains, "epistemology is concerned primarily with knowledge acquisition and development, doctrine is understood to play an inherently epistemological role within the military institutions that produce it."[71] Doctrine seeks to teach or train through the acquiring of knowledge establishing an epistemology relationship. Theory "then becomes a guide to anyone who wants to learn about war from books; it will light his way, ease his progress, train his judgment, and help him to avoid pitfalls."[72] ULO provides the cognitive link between strategy and tactics, furnishing the guiding light through a common belief system and the necessary knowledge needed prior to conducting operations, in order to avoid common mistakes. Thus serving as the theory and overarching doctrine for all US Army operations.

Unified Land Operations acknowledges the importance of all domains, to include cyber, when describing the overarching strategic context and operational environment in which the Army will operate. ULO describes the operational environment as a "composite of conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[73] The operational environment is described by two sets of variables; mission—Political, Military, Economic, Social, Information, Infrastructure, Physical environment, Time (known as PMESII-T) and operational variables—Mission, Enemy, Terrain and weather, Troops and support available, Time available, Civil considerations (known as METT-TC). The variables are used to evaluate each specific operational environment and the relationship between them and each domain, to define the unambiguous state, within each unique

[71]Jackson, 7.

[72]Clausewitz, 141.

[73]Department of the Army, Army Doctrine Publication 3-0, 2.

operational environment. ULO states that one way enemy forces may attempt to disrupt operations, in an operational environment is through "cyber-attacks."[74]

Unified Land Operations provides the framework, which all doctrine must support. As the capstone document, ADP 3-0 defines the Army's overarching belief system and body of thought for how it will conduct land combat operations. Thus, ULO is not only the capstone doctrinal publication but is also the theoretical foundation for developing other principles, tactics, techniques, and procedures through subsidiary doctrinal publications.[75] Since ULO provides the necessary theoretical and doctrinal principles applicable to all Army operations, cyberspace doctrine must integrate into the Army's existing doctrinal structure.

The United States Army's Cyber Doctrine Journey

The US Army published its first doctrinal manual that addressed cyberspace operations (CO) in February 2014, FM 3-38, *Cyber Electromagnetic Activities*. Prior to its publication the Army embarked on a four year journey to define and develop FM 3-38. Two specific publications influenced and continue to forward the cyber doctrinal discourse, Training and Doctrine Command (TRADOC) Pamphlet 525-7-8, *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028,* and the Army's *LandCyber White Paper*. The development of doctrine is important since it provides the "common philosophy, language, purpose, and unity of effort," but, it maybe even more relevant in the quickly developing domain of cyber, since very little operational experience exists within the force.[76]

---

[74]Ibid., 4.

[75]Ibid., ii.

[76]COL(R) Clinton J. Ancker III and LTC (R) Michael A. Scully, "Army Doctrine Publication 3-0: An Opportunity to Meet the Challenges of the Future," *Military Review* (January-February 2013): 38.

In February 2010, the Army published TRADOC Pamphlet 525-7-8, its purpose was to "develop a common understanding of how technological advancements transform the operational environment, how leaders must think about cyberspace operations, how they should integrate their overall operations, and which capabilities are needed."[77] The pamphlet sought to describe the operational environment, determine the problems, and provide solutions under the Army's doctrine, organization, training, material, leadership and education, personnel, and facilities (also known as DOTMLPF) construct.

TRADOC Pamphlet 525-7-8 looked at how the Army can leverage cyberspace from 2016-2028 and serve as the embarkation point for future doctrinal development.[78] It outlines how commanders could integrate cyber operations to gain an advantage, protect that advantage, and place adversaries at a disadvantage.[79] Cyber operations are defined as "the employment of cyber capabilities where the primary purpose is to achieve objectives in and through cyberspace."[80] The pamphlet also highlights, that the relationships between all the domains to include cyberspace, are interdependent, along with the growing importance of contested space in the electromagnetic spectrum. Most importantly, the pamphlet began to develop a common vocabulary for Army CO.

Three main recommendations were produced in TRADOC Pamphlet 525-7-8 that centered on the need to better posture the Army for the integration of CO in the future. The first recommendation concluded that the current vocabulary for cyber, electronic warfare, and information operations was adequate but would grow increasingly inadequate as the operational environment changes. Second, three dimensions exist when addressing CO and each requires

---

[77]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, ii.

[78]Ibid., iii.

[79]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, iv.

[80]Joint Chiefs of Staff, Joint Publication 1-02, 68.

force and doctrinal solutions. Lastly, the Army should progress from the terms cyber, electronic warfare, and information operations to describe them as the first, second, and third dimensions.[81] The shift to a dimensional focus would encapsulate all three as a way of achieving objectives through various means. The first dimension would center on the contest of wills, the second dimension on strategic engagements, and the third dimension on the cyber-electromagnetic contest. While TRADOC Pamphlet 525-7-8 primarily focused on prevailing in the third dimension, cyber operations enables the first two dimensions.[82]

Understanding that the cyber domain directly enables or inhabits operations on land, the Army admitted that it "does not have a holistic vision, concept, or doctrine to guide its capability development efforts in response to the changes in the operational environment (OE) and operational requirements for cyber operations."[83] The Army recognized that the development of a complete approach in the cyber domain is imperative. As such, TRADOC Pamphlet 525-7-8 stated,

> The art of winning in the cyber-electromagnetic dimension requires very specific expertise in information theory, computer science, and related sciences (electro-physics, radio-electronic wave propagation theory, cyber-electronics, complex cyber network

[81]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, 15-16. On 16 October 2009, the CG TRADOC provided recommendations to the Army, Vice Chief of Staff. Included among his recommendations were the following: (1) The Combined Arms Center determined that current vocabulary (cyber-Electronic Warfare-Information Operations) is adequate today, but will become increasingly inadequate to describe the challenges the Army faces in the operational environment. (2) The Combined Arms Center concluded that there are three dimensions to be addressed, that these dimensions exist across the Full Spectrum Operations, and that these dimensions each require force design and doctrinal solutions. (3) Therefore, although the Army currently describes the functions related to network and spectrum operations as cyber-Electronic Warfare-Information Operations, the Combined Arms Center believe that the Army should adapt and describe them in the future as follows: First dimension—the first dimension is the psychological contest of wills against implacable foes, warring factions, criminal groups, and potential adversaries. Second dimension—the second dimension is strategic engagement and involves keeping friends at home, gaining allies abroad, and generating support or empathy for the mission in the area of operations. Third dimension—the third dimension is the cyber-electromagnetic contest. Trends in wired, wireless, and optical technologies are setting conditions for the convergence of computer and telecommunication networks.

[82]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, iv.

[83]Ibid., 14.

> behaviors, and others) and of how this theoretical knowledge relates to military tactics, operations, and strategy. Creating this marriage of abstract science and modern military practice is fundamental to creating cyber operations situational awareness and thus contributing to the commander's end state.[84]

Although "winning" may be a miss leading term to use in the context of the constantly contested domain of cyberspace. The acknowledgement of a holistic approach to address the complexity of cyberspace, serves as a significant starting point to develop relevant cyber doctrine. It also supports the national strategic guidance and DoD's cyber strategy to provide a whole of governance and civilian partnership approach. The importance of understanding all the necessary expertise which is required in cyberspace highlights the technological and social aspects that converge in the cyber domain. The combining of cyber and electromagnetic into one activity is an attempt to show the interdependency that exists between the two.

The next significant evolution of US Army cyber doctrine was *The US Army LandCyber White Paper 2018-2030*, published in September 2013, which superseded TRADOC Pamphlet 525-7-8. The *LandCyber White Paper* continued to further define the problem and potential solutions for conducting operations in the cyber domain; describing the dependence and reliance of cyberspace on all Army operations, and that the threat from state and non-state actors will "continue to evolve and proliferate."[85] The *LandCyber White Paper* frames the institutional solution for the Army by "describing a transformational concept that deals with emerging cross-domain dynamics, land and cyberspace, while accounting for fundamental changes in the operational environment."[86] Through the development of an operational outcome similar to the AirLand doctrine of the 1980s it "will ensure optimal integration of land and cyber effects to

---

[84]Ibid., 17.

[85]Army Cyber Command/Fort Meade MD Army (2nd), *The US Army LandCyber White Paper 2018-2030* (Fort Meade, MD: US Army Cyber Command/2nd US Army, 9 September 2013), v.

[86]Ibid.

influence the threat before it impacts friendly forces and operations," through the development of the LandCyber concept.[87]

Although cyberspace's cross domain characteristics may appear intangible, it is that intangibility that relates cyber to the abstractness of doctrine, since "doctrine is somewhat abstract, but provides the foundation from which to begin thinking when facing a concrete and specific decision."[88] While LandCyber sought to further the discussion for a doctrinal foundation in cyberspace, the new conceptual idea required further explanation.

The LandCyber concept consists of, "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."[89] It is the Army's transformation concept that accounts for the emergence of cyberspace on the traditional land domain, striving to apply global thinking to actions that occur locally.[90] Thus in some aspects the LandCyber concept is the Army's first effort to provide cyber theory in order to create supporting doctrine.

The *LandCyber White Paper* calls on four roles and responsibilities for the Army to effectively operate in cyberspace. First, it must "support prevent, shape, and win roles with cyberspace capabilities." Second, it must "provide critical infrastructure protection for the Army and US Northern Command national systems." Third, "integrate cyberspace operations capabilities into joint and Army planning exercise." To include the development of a "world-class cyber opposing force." Finally, to "integrate cyberspace operations into combatant command

---

[87]Ibid., vii.

[88]COL Dennis M. Drew and Dr. Donald M. Snow, *Making Strategy: An Introduction to National Security and Process and Problems* (Maxwell Air Force Base, AL: Air University Press, August 1988), 172.

[89]Army Cyber Command/Fort Meade MD Army (2nd), 43.

[90]Ibid., iii-iv.

planning and targeting," and "deliver offensive and defensive cyber effects." The Army Cyber Command is the Army's service component to the United States Cyber Command, tasked to develop operating concepts that nest within Joint Cyberspace Operations to accomplish the roles and responsibilities.

The declaration of cyberspace as a domain has elevated the strategic importance of cyberspace but also added consequences to the strategic importance of operating in the domain. The LandCyber concept states that the domains, (land, air, sea, space and cyber), are critical to project power in order to have "access to the world and its resources."[91] In order to have power in the cyber domain there must be reconciliation with the physical and cognitive dimensions with the emergence of the virtual dimension. "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."[92] The relationship between the three dimensions provides the understanding of how to see and describe the operational environment, along with the influence of the actions of people and machines.

The LandCyber White Paper redefines the three dimensions in TRADOC Pamphlet 525-7-8 from a contest of wills, strategic engagement, and cyber-electromagnetic to the physical, information environment (cognitive), and virtual dimensions. The virtual dimension, cyberspace, is the tool that enables the movement between the physical and cognitive dimensions. This description of the operational environment recognizes that land is where humans primarily operate to interchange between the three dimensions.[93]

---

[91]Ibid., 6.

[92]Ibid., 7.

[93]Ibid.

In order to address the problem of merging land and CO, *The LandCyber White Paper* carried forward from TRADOC Pamphlet 525-7-8 the solution framework to account for eight aspects of convergence and nine guiding principles (table 1).[94] The eight aspects of convergence seek unifying effects of cyberspace and land operations, with principles to explain their implementation, to the organization to deliver an integrated warfighting platform to enable success in the Army's prevent, shape, and win roles.[95]

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

Source: Army Cyber Command/Fort Meade MD Army (2nd), *The US Army LandCyber White Paper 2018-2030* (Fort Meade, MD: US Army Cyber Command/2nd US Army, 9 September 2013), viii.

The eight aspects of convergence point back to the inherent problem of the cyber domains creation and domain name. Relationships are acknowledged with interdependency between each aspect. All of which are moving together to create something more than a domain. The collusion of domains and environments are occurring to create a sphere of influence. Allen

[94]Ibid., viii.

[95]Ibid., 23.

and Gibson's term, Information Sphere, more accurately incorporates the relational existence of eight aspects of convergence.

In February 2014, the Army published FM 3-38, *Cyber Electromagnetic Activities* (CEMA). It is the first field manual to specifically address CO and its inherent relationship within the electromagnetic spectrum. The feature purpose of FM 3-38 "is to provide an overview of principles, tactics, and procedures on Army integration of CEMA as part of unified land operations."[96] As a field manual, FM 3-38 focus on principles, tactics, and procedures but by its own admission provides only "enough guidance for commanders and their staffs to develop innovative approaches to seize, retain, and exploit advantages throughout an operational environment."[97] However, it does provide much needed definitional clarification and actions in support of ULO.

By placing CEMA at the Field Manual level, the Army's third hierarchal doctrinal tier, it relegates the importance of CO. Since cyber now constitutes a domain, the conceptual idea of CO may better serve along the Army's first tier of doctrinal manuals at the Army Doctrine Publication level. As an Army Doctrine Publication, FM 3-38 would elevate the importance of understanding how CEMA makes an impact across the entire operational environment, and better demonstrate how convergence is occurring across multiple domains and influences all operations.

Field Manual 3-38 builds upon the relationships established in the LandCyber concept through defining CEMA as the integration and synchronization of the functions and capabilities of CO, electronic warfare (EW), and spectrum management operations (SMO).[98] The interdependency between cyberspace and the electromagnetic spectrum emerged in TRADOC

---

[96]Department of the Army, Field Manual 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Headquarters Department of the Army, 12 February 2014), v.

[97]Ibid., iv.

[98]Ibid., 1-2.

Pamphlet 525-7-8 and became formalized in doctrine with the term CEMA. The three components of CEMA; CO, EW, and SMO display unique characteristics, that in order to maximize their potential and effectiveness they must be synchronized and integrated through Cyber Electromagnetic Activities in order to fully support Unified Land Operations.[99]

Recognizing that the operational environment has changed drastically with the addition of the cyber domain, FM 3-38 uses CEMA to expand the Army's situational understanding and knowledge of the interdependency between all relevant relationships that occur both internally to cyber and externally with the traditional four domains. CEMA adds to and defines the important relationship of the EMS, which like the four traditional domains exists naturally. While the man-made domain of cyber is connected to the physical domains by its infrastructure, movement in the domain is enabled through the EMS. This provides a physical residence of cyberspace through its components in the natural domains, as displayed in figure 2.[100]

[99]Ibid., 1-3.

[100]Ibid., 1-4.

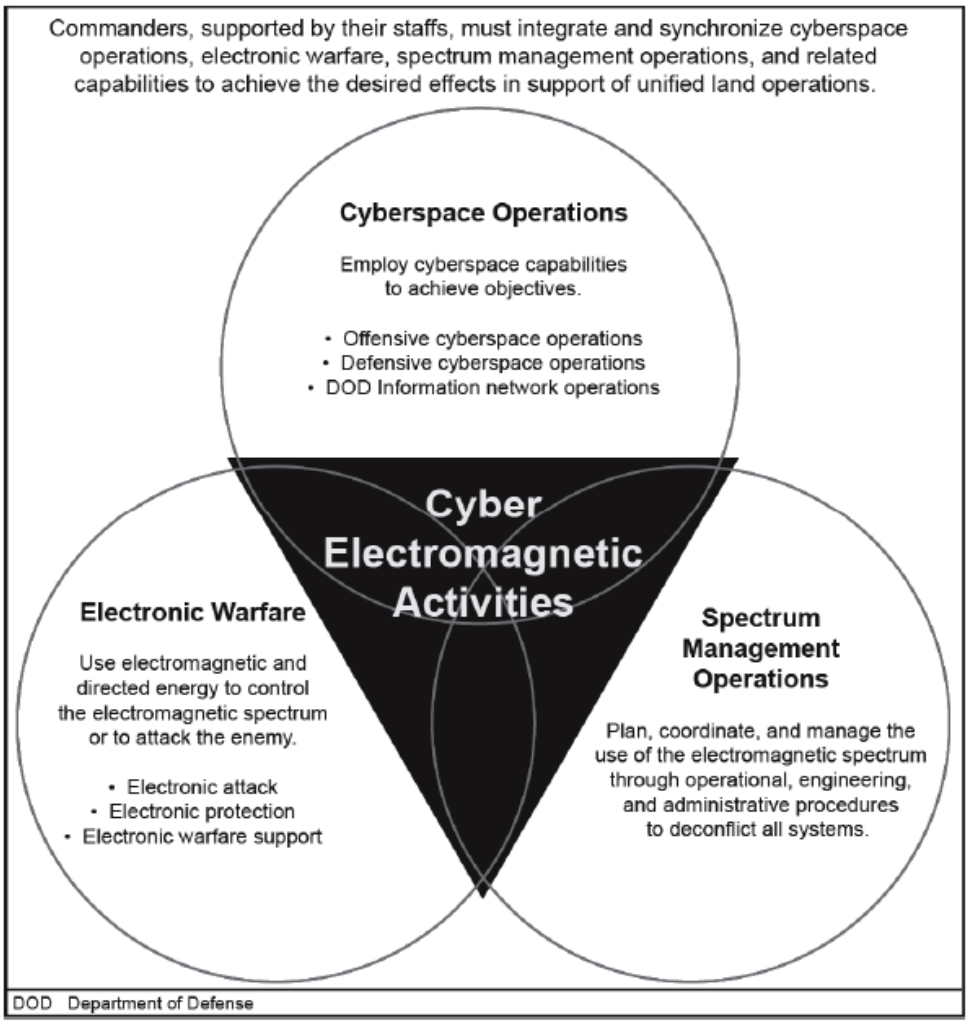

Figure 2. Cyber Electromagnetic Activities

Source: Department of the Army, Field Manual 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Headquarters Department of the Army, 12 February 2014), 1-2.

While the CEMA concept is a move forward from solely looking at cyberspace as a single system, the relationship with SMO shows how cyber interacts with the space domain. In the electromagnetic spectrum, cyber and space overlap in order to permit the transfer of information, by means other than hardwire infrastructure. FM 3-38 acknowledges the cyberspace

and space domain relations stating they "are uniquely and interrelated primarily because of their current role in telecommunications and networks."[101] The components that enable this to occur for the cyber domain exist in all the domains to include space, but travel from one component to another through the EMS, which resides in the space domain. The relationships among the five domains and electromagnetic spectrum (figure 3) draws a distinctive line between cyberspace and the EMS, but the EMS exists throughout the earth and beyond. The interaction between cyber and the space domains lend more to the environment description in both their definitions. This further contributes to the problem of creating the cyber domain and labeling it as such, without looking holistically at the problems that need to be solved prior to action.

[101]Ibid., 1-5.

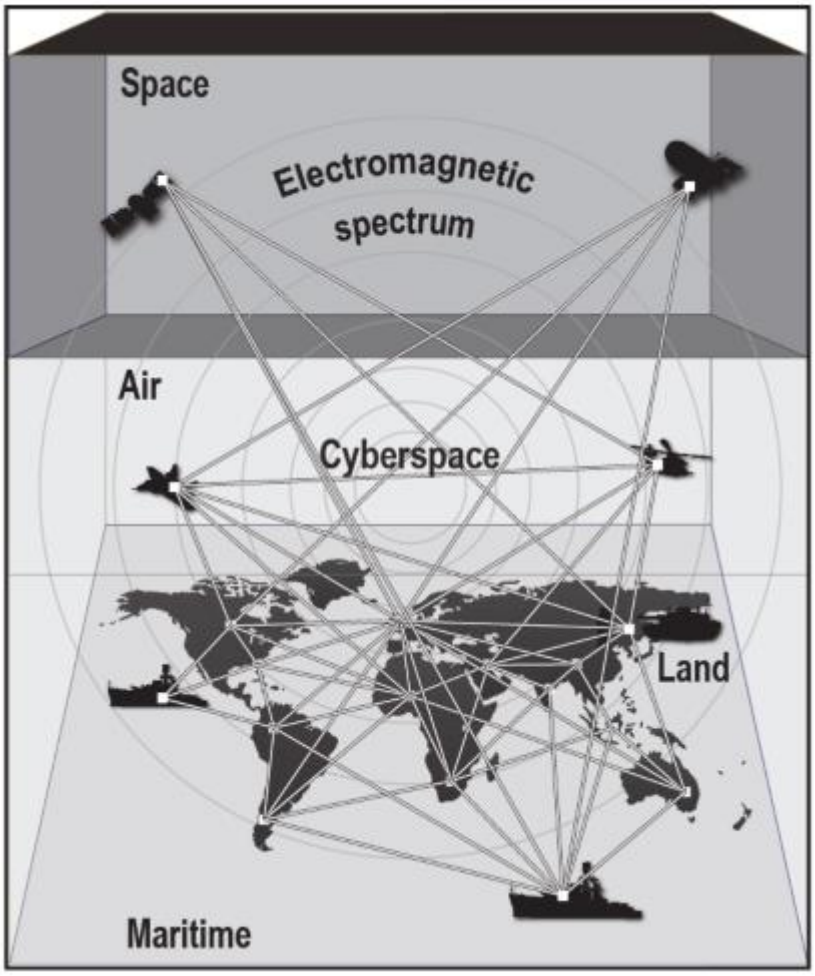

Figure 3. The Relationships among the Five Domains and Electromagnetic Spectrum

Source: Department of the Army, Field Manual 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Headquarters Department of the Army, 12 February 2014), 1-4.

Although cyberspace shares a relationship with the other domains, it also displays unique characteristics that differentiate it from the others as well. Perhaps one of the most telling acknowledgements of cyberspace in FM 3-38 is that it describes it as a "system of systems."[102] By recognizing that cyberspace is a system of systems, the Army acknowledges that cyberspace

[102]Ibid., 1-5.

is complex and open to feedback from the environment that it operates.[103] The influences on the system are driven by non-government industries with constant changing technology. This constant change solidifies emergent behavior that is tied to a spatial or geographical point which creates a shift from the paradigm of effects on objectives, to the ability to capitalize on dominating information to a higher degree of importance.[104]

Field Manual 3-38 specifically states that cyberspace characteristics are significantly different form the land, air, maritime, and space domains.[105] To adequately address the uniqueness of cyberspace more is required than simply integrating and synchronizing CO, EW, and SMO operations in CEMA. While understanding the relationship between CO, EW, and SMO is important, the simple naming of the group as CEMA downplays the importance of the combined effects that all three have as an operation versus an activity. The concept of creating CEMA to define the relationship between cyberspace and EMS highlights the confusion of the creation of the fifth domain and calling it cyberspace. If cyberspace is the domain then it should be the overarching concept to "provide commanders with the ability to gain and maintain an advantage in cyberspace and EMS."[106]

While each sub system of CEMA; CO, EW, and SMO are operations, integration and synchronization occurs through the activity of CEMA. The construct of CEMA as an activity misinforms the act that needs to occur in cyberspace. The operation is the integration of CO, EW,

---

[103]Alex J. Ryan, "What Is a Systems Approach?," http://arxiv.org/abs/0809.1698 (accessed April 1, 2014), 2. System—A system is a bounded region in space-time, in which the component parts are associated in functional relationships.

[104]Mark W. Maier, "Architecting Principles for Systems-of-Systems," *Systems Engineering* 1, no. 4 (1998): 267-284. System of systems Distinguished from large but monolithic systems by the independence of their components, their evolutionary nature, emergent behaviors, and a spatial or geographic extent that means information exchange is more important than flows of matter or energy.

[105]Department of the Army, Field Manual 3-38, 1-5.

[106]Ibid., 1-3.

and SMO, along with all other types of operations. An operation implies power and influence while an activity is at best an action. Though dominance in cyberspace may not be attainable, the projection of power and influence certainly is obtainable. The Army's creation of CEMA as an activity can be linked to the poor naming of the cyber domain. CEMA attempts to address the complexity of cyberspaces as a system of systems, but does not go far enough to fully describe and define the interdependence of the sub systems in the overarching system.

Part of the uniqueness of the cyber domain rests in the notion that it is man-made. Since its components are man-made, they will constantly evolve and be every changing. The rate of change in its components poses an interwoven relationship between the technology and doctrinal development of cyberspace. Any cyber doctrine must be tied to principles that are formed in the advancements of technology. The interconnectedness between technology and doctrine development will provide guiding principles to further enhance the ability to fight from and in the cyber domain.

Field Manual 3-38 seeks to capitalize on the ability to fight from and in the domain through the integration of CO, EW, and SMO. Although conceptualizing the cyber domain as a war fighting domain is challenging, the lack of a grand theorist or theory does not limit the Army's ability to integrate CO. Unified Land Operations serves as the Army's guiding theory of warfare and provides the agility to integrate supporting cyber doctrine. While FM 3-38 introduces and solidifies cyber domain terms and definitions, a key component of doctrine, the placement of the Army's new operating concept of CEMA in a field manual, the Army's third tier of doctrinal hierarchy, dilutes the importance of the cyber domain.

CYBERSPACE OPERATIONS AND FIELD MANUAL 3-38

FM 3-38's description of CO impacts three tenets of Army operations that significantly affect operations in cyberspace: synchronization, integration, and depth. These three tenets focus on the effects of time, space, and purpose, which directly influence operational art. By looking at

a cyber-attack as solely, one attack to achieve a specific effect may be missing the ability to grasp the potential of CO. Cyberspace operations flatten the levels of war; strategic, operational, and tactical through their ability to achieve strategic objectives through tactical means that are unique to cyberspace.

In September of 2007, Israel launched an air strike against a Syrian nuclear facility. Although there was initial dispute regarding whether the target attacked was actually a nuclear weapons plant, later intelligence confirmed the target was a North Korea designed facility. Nevertheless, the story behind the attack was not that Syria was building a nuclear weapons plant. Rather, it was about how Israel was able to conduct such an aerial attack deep into Syria without detection, against a country that spends billions of dollars on air defense. Although it is not exactly known how the Israeli's blinded Syria's air defense system, it has to be credited to a form of cyber-attack that disrupted the Syrian's air defense network. The Syrian's saw no aircraft or any sign of a pending attack on any of their air defense systems. Somehow, the Israeli's were able to gain access and blinded the Syrian's air defense systems to display no physical signs of any aircraft within their borders.[107]

Israel was able to integrate and synchronize effects in cyberspace with a traditional air attack to facilitate movement, achieve surprise, and increase chances for success through an arrangement of tactical actions in time and space, to achieve a strategic goal through fighting from cyberspace. Israel successfully demonstrated the ability of synchronization and integration of capabilities and effects through extending operational art to cyberspace. Operational art is the cornerstone of Army planning that bridges the gap between strategic objectives and tactical actions. ADP 3-0 defines operational art as "the pursuit of strategic objectives, in whole or in

[107]Clarke and Knake, 1-8. Richard Clarke describes the Israeli attack against Syria to prevent Syria from building a nuclear weapons plant.

part, through the arrangement of tactical actions in time, space, and purpose."[108] Commanders apply operational art to "balance risk and opportunity in order to create and maintain the conditions necessary to seize, retain, and exploit the initiative and gain a position of relative advantage while linking tactical actions to reach a strategic objective."[109] Three of the Army's tenets of operations; synchronization, integration, and depth can be uniquely applied in CO to facilitate operational art in new and distinct ways. The ability to grasp how cyberspace is changing aspects of the operational environment will better enable commanders to maximize all aspects of time and space to achieve desired purposes.

If expectations are necessary before developing strategy an argument arises; what comes first strategy or tactics? Lukas Milevski argues in his article, "Strategy and Cyberpower: From Tactics to Politics," that tactics drive strategy since strategy is irrelevant if it cannot be achieved by the available means of the actor imploring it. In the traditional sense of warfare in a physical domain, "strategy directs the employment of power in adversarial situations for political ends; tactics are what actually make that power work."[110] However, in cyberspace the traditional approach of the levels of war; strategic, operational, and tactical become flattened. Edward Luttwak explains, "cyberspace compresses aspects of strategic hierarchy . . . the logic of strategy works on, and melds together, all levels of agency in war from the technological to the tactical, the operational, the strategic, and the grand strategic."[111] Milevski goes on to describe that in the four physical domains tactics adapt to and exploit technology, while the human dimension

---

[108]Department of the Army, Army Doctrine Publication 3-0, 9.

[109]Ibid.

[110]Lukas Milevski, "Strategy and Cyberpower: From Tactics to Politics," *Infinity Journal* 3, no. 2 (Spring 2013): 18, https://www.infinityjournal.com/article/96/Strategy_and_Cyberpower_From_Tactics_to_Politics/ (accessed December 26, 2013).

[111]Ibid.

remains constant. Nevertheless, this is not necessarily the case in the cyber domain; in cyberspace technology adapts to exploit tactics.

Conducting operations in cyberspace and using cyberpower may compress strategy and tactics even closer together. Tactics in cyberspace begin at the point of entry. A person enters cyberspace through the physical layer of cyberspace (computer) then maneuvers through the logical layer (servers, web address) before reaching its intended target back in the physical layer. While soldiers in the physical domains use technology to facilitate their tactics, in cyberspace the technology becomes part of the tactics, since technology drives changes to such things as software and programs and thus influences doctrine application.[112] This close knit relationship between strategy and tactics displays the effects that operations in cyberspace can obtain. While cyber doctrine does not correspond to a specific theorist, it does nest within ULO. However, as a domain, the nature of cyber has the ability to close the gap between strategy and tactics.

If CEMA's purpose is the integration and synchronization of the functions and capabilities of CO, EW, and SMO, it does not address the impacts on time and space in cyberspace.[113] Integration and synchronization are not only key buzzwords that apply to CEMA but are two of the Army's six tenets of operations. Synchronization defined in JP 1-02 as "the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place in time." FM 3-38 only discusses time in the context of planning and

---

[112]Milevski, "Strategy and Cyberpower: From Tactics to Politics," 19. Unlike on the sea, in the air, or in orbital space, in cyberspace technology and tactics are virtually synonymous. In the four warfighting domains, tactics adapt to and exploit technology while the human dimension remains constant. Soldiers on the ground execute the tactics using whatever technology is readily available and may make adjustments if the situation warrants. By contrast, the use of technology for cyberpower begins at the point of access to cyberspace. Thereon, most activity, including tactics, depends on pre-programmed software and the expertise to modify programs ad hoc and in the heat of the moment. A program thus simultaneously represents both a particular tactical capability and a specific tactical doctrine, for it combines with what is instead of how it is achieved. This results in an actual conflation of means and ways in strategy, creating what might be considered as pure a context as possible (short of the abstractions of nuclear strategy) for considering the relationship between tactics and strategy.

[113]Department of the Army, Field Manual 3-38, 1-2.

preparing to conduct cyber operations and the shared relationship between cyber and space domains. It does not discuss the impacts of how time and space have been altered to achieve a purpose from cyberspace. TRADOC Pamphlet 525-7-8 stated that CO are able to affect the operational environment near instantaneously with a speed that cannot be achieved through the other domains.[114] Although now rescinded, TRADOC Pamphlet 525-7-8's recognition of changes in perception of time provides initial insights and understanding, but further development of how time and space have changed in cyberspace still needs to occur.

Adrian Mihalache's essay, "The Cyber Space-Time Continuum: Meaning and Metaphor," addresses the unique relationship between time and space in cyberspace. Mihalache refers to cyberspace as "cyberspace-time" and that it is not a void waiting to be filled but rather an aggregation of places or sites.[115] In it, "space is created together with time in the act of finding places in cyberspace." The spatial and temporal synthesis meets to focus past experiences and create new ones. Time becomes the currency of cyberspace. Mihalache uses the term cyberspace-time to better portray the domain of cyberspace describing it as predominately an information discourse realm. Information is readily available and it becomes a fight to maintain your attention at a particular site. The attention that is given to a particular site is the transfer of time. Although time or your attention is given to one site it may not and does not have to be mutual. Discourses may never meet; just pass by each other until someone's time meets another in a particular site simultaneously.

Even if operations occur without interference in cyberspace it does not mean that they were not observed. Time and space do not have to meet in order for two belligerents to conduct a meeting engagement and there is no requirement for acknowledgement by either party. Freedom

---

[114]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, 10.

[115]Adrian Mihalache, "The Cyber Space-Time Continuum: Meaning and Metaphor," *Information Society* 18, no. 4 (July 2002): 293.

of maneuver does not mean freedom from observation. The very structure of cyberspace implies that it is vulnerable to attack or intrusion. The US military's network structures are not exempt since their architectural framework relies on civilian infrastructure.[116] The mindset in operating in cyberspace must expand to include simultaneously conducting offensive, defensive, and sustaining operations all at the same time.

No longer does synchronization apply to only one operation at a time. It now requires synchronization of multiple operations simultaneously, in order to integrate effects across the range of cyber operations to achieve strategic objectives. Figure 4, FM 3-38's three independent functions of CO, depicts and defines the three functions that occur in CO and their interrelationship. The circles, as a graphical depiction are a good choice; however the picture and name of independent functions, implies that offensive cyberspace operations, defensive cyberspace operations, and information network operations are independent of one another and only intersect at certain times and spaces.

[116]US Army Training and Doctrine Command, TRADOC Pamphlet 525-7-8, 16. The US Army is heavily reliant on information technology and information systems to communicate, control forces, coordinate fires, gather and distribute intelligence, and conduct surveillance, reconnaissance, and other military activities. US adversaries, warring factions, and criminal cartels have access to and use many of the same technologies in innovative ways that are unique to every case.

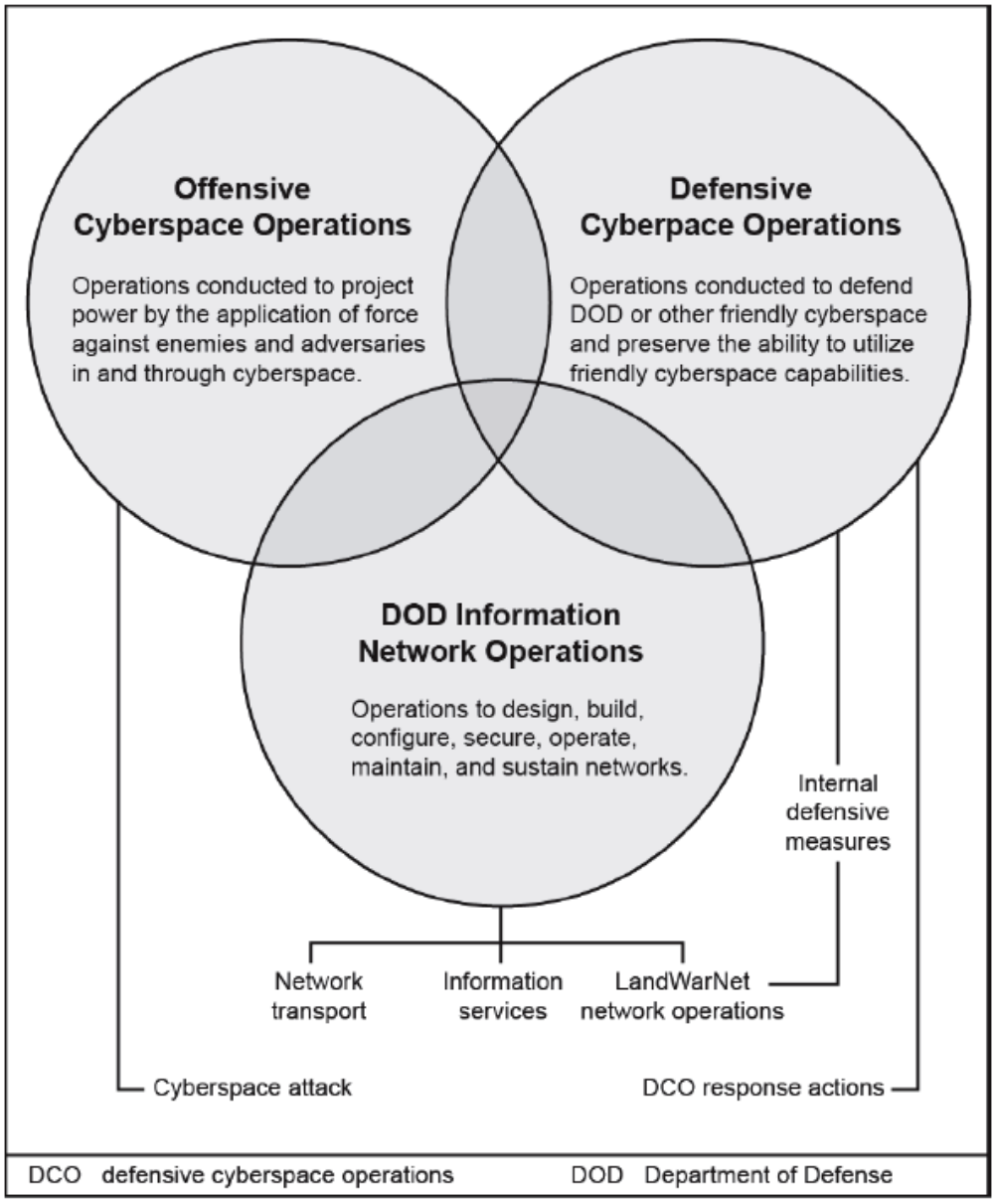

Figure 4. The Three Independent Functions

Source: Department of the Army, Field Manual 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Headquarters Department of the Army, 12 February 2014), 3-2.

The implication is that all three functions are autonomous and are only intersecting at specific moments in time and space. Perhaps a better graphical depiction would be a layered approach that illustrates all three circles assimilating into each other, advancing the idea that the

time spent in one layer may transfer to a space in another, as pictured in figure 5. This would also help to better graphically depict the system of systems approach in cyberspace. The idea behind the three overlapping circles with depth and dimension is to correspond to the layered description of cyberspace and the dimension description of the information environment. This shows that all three functions occur simultaneously versus distinctively between operations, along with how the time and space relationship has changed in cyberspace. The two tenets of synchronization and integration must occur internally to CO, while simultaneously with other operations in the physical domains.

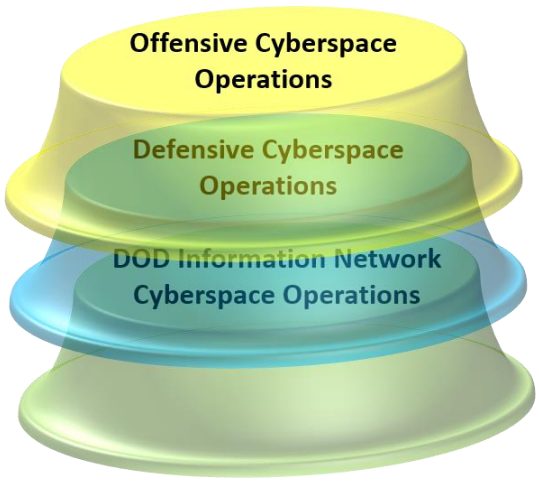

Figure 5. The Integrated Functions of Cyberspace Operations

Source: Created by author.

Applying synchronization and integration both internally and externally facilitates FM 3-38's employment of a cyberspace attack. FM 3-38 states, "cyberspace attack capabilities are employed to support maneuver operations by creating simultaneous and complementary

effects."[117] In order to grasp the simultaneous and complementary effects FM 3-38 defines the capability of a cyberspace attack as a: "capability may be employed in conjunction with electronic attack, offensive space control, fires, and information related capabilities to deceive, degrade, destroy, and disrupt a specific enemy integrated air defense system or enemy safe haven."[118] The capabilities of a cyber-attack provide a great example of the third tenet of Army operations that addresses time and space, depth.

The tenet of depth and CO are designed to complement one another. Often depth is misunderstood in conventional aspects of the battlefield in a linear notion. Depth is the extension of operations in space, time, or purpose achieved by ULO when the enemy must cope with actions throughout its entire physical, temporal, organizational depth.[119] In cyberspace, depth applies to the cognitive information environment and network of technology that exists in the cyber domain. To achieve depth in cyberspace, capabilities must exist to enable the ability to fight in the domain across all layers of cyberspace and the information environment, while simultaneously defending the network that it is operating from.

Depth combined with synchronization and integration enables the entire enemy system and its components to be attacked either in isolation or together with physical actions. In 2007, Russia conducted a two-phase attack against Estonia. The first phase knocked out government

---

[117]Department of the Army, Field Manual 3-38, 3-3.

[118]Ibid., 3-3.

[119]Department of the Army, Army Doctrine Publication 3-0, 8. Depth is the extension of operations in space, time, or purpose. Army leaders strike enemy forces throughout their depth by arranging activities across the entire operational framework to achieve the most decisive result. They do this to prevent the effective employment of enemy reserves, command and control nodes, logistics, and other capabilities both in and out of direct contact with friendly forces. Unified land operations achieves the best results when the enemy must cope with US actions throughout its entire physical, temporal, and organizational depth.

web servers and news sites. The second phase consisted of a botnet[120] which involved 178 countries' critical infrastructure. While the cyber-attacks were conducted, a physical aspect also occurred simultaneously, which consisted of flash mobs that disrupted traffic, caused roadblocks, and some physical attacks against Estonia parliament members.[121] Estonia provides an example of how the concept of depth can attack the physical, temporal, and organization of an enemy concurrently or in a successive manner.

Russia's attack on Estonia and Israeli's attack on Syria provide examples of how a cyberspace attack was used to facilitate a physical attack. FM 3-38 states that a cyberspace attack "consists of actions that create various direct denial effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains."[122] FM 3-38's definition of a cyberspace attack is similar to Daniel Bilar's nth Order Attacks. Bilar describes an nth Order Attack as an attack that "tries to indirectly degrade, disable or subvert an end system by targeting one or more ancillary systems."[123] Bilar's nth Order Attack seeks to target the ancillary parts that make up the system that are responsible as the mechanisms of control. Ancillary systems make up the system and range in levels of complexity.[124]

An attack does not need to come straight at the system, but through attacks at the sub systems or components that make up the system. Ancillary attacks could be directed towards the

---

[120]"Bot (from robot) networks or botnet are made up of vast numbers of computers that are infected and remotely controlled to operate, in concert, through commands sent via the Internet. They are used to block or disrupt the computers of targeted organizations or to distribute spam, viruses, or other malicious code." Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, DC: Center for Technology and National Security Policy, 2009), 420.

[121]Czosseck and Geers, 271.

[122]Department of the Army, Field Manual 3-38, 3-3.

[123]Czosseck and Geers, 265.

[124]Ibid., 263.

entry and exit ports in the information sphere. Attacking the ancillary components that open the network at the entry and exit points of the system seeks to exploit vulnerabilities and attempt to gain control at specific places and time in cyberspace. Bilar's usage of the terms degrade, disable, or subvert are similar to FM 3-38's descriptive words of degradation, disruption, or destruction. One thing that is missing in both definitions is dominate. Degrading, disrupting, and destruction of certain components are much more achievable in cyberspace, versus the attempt to dominate an entire domain that encompasses a global environment and facilitates temporal and spatial control.

Field Manual 3-38 describes the ability to "gain and maintain freedom of action in cyberspace through achievement of periods of cyberspace superiority."[125] Cyberspace superiority, as defined in JP 1-02, states that superiority is "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."[126] The connotation of superiority in cyberspace defaults to the idea of dominance and may be a side effect of making cyber a domain. However the recognition that superiority can be achieved for a given time and place better captures how time and space are changed in cyberspace and can be tied to the tasks of degrading, deceiving, disrupting, and destruction.

Seeking to achieve effects through tasks such as degrading, deceiving, disrupting, and destruction in cyberspace advances another issue. Should the Army's tactical doctrinal taxonomy be expanded to include information capability terms since they may now also apply to cyberspace operations? The Army's tactical taxonomy chart (figure 6) in Army Doctrine Reference Publication 3-90, *Offense and Defense*, lists three major components: elements of decisive action

---

[125]Department of the Army, Field Manual 3-38, 3-1.

[126]Joint Chiefs of Staff, Joint Publication 1-02, 70.

and three subordinate tasks, tactical enabling tasks, and tactical mission tasks. Adding deceive and degrade to the tactical mission tasks and denial to the tactical enabling tasks of the Army's tactical doctrinal taxonomy would provide doctrinal tasks that could be applied to cyberspace operations. This may even influence the traditional relationship between task and purpose through incorporation of simultaneous and complementary effects.

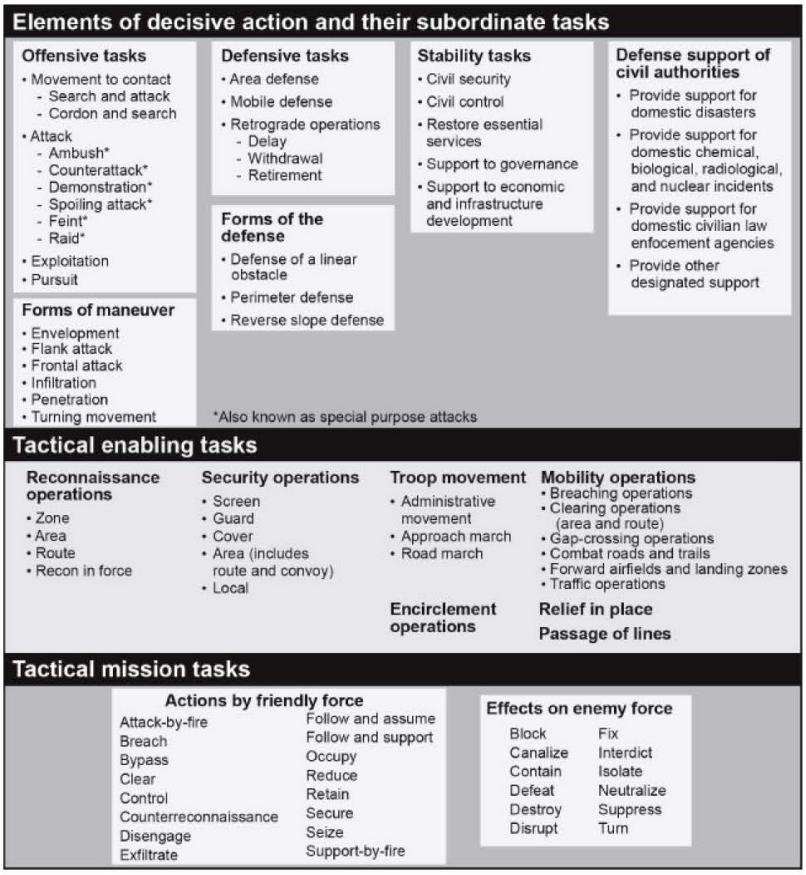

Figure 6. Army Tactical Doctrinal Taxonomy

Source: Department of the Army, Army Doctrine Reference Publication 3-90, *Offense and Defense* (Washington, DC: Headquarters Department of the Army, 31 August 2012), 2-3.

Cyberspace operations transcend all domains and while ULO provides the Army's operating theory of warfare, the addition of cyber as a domain creates doctrinal impacts. "The

inclusion of cyberspace and the EMS greatly expands and complicates the operational framework, transforming a limited physical battlefield to a global battlefield."[127] While operational art still applies to operations in cyberspace and the Army's tenets of operations remain relevant, CEMA has impacts that influence all Army operations. The placement of CEMA as a field manual in the Army's third level of doctrinal hierarchy may not be giving the doctrinal importance and relevancy to CO. The convergence of the levels of war in the cyber domain are significant enough for the Army to raise CEMA to an ADP document to further define and explain the fundamental principles of CEMA and time, space, and purpose relationships in the cyber domain.

CONCLUSION

The current Army doctrinal construct for cyber operations is insufficient to meet emergent threats and keep pace with constant rapid technology growth. To substantiate this argument the monograph explored three key areas. The first section defined cyberspace and domain, to include the impacts of raising cyber to the domain level. The second section examined the impacts of technology in the development of cyber doctrine and if the lack of a prescribed cyber theory would hinder doctrinal development. This included the journey of the development of the Army's first doctrinal publication that addressed the cyber domain, FM 3-38. The final section scrutinized the understanding and impacts that CO had on three of the Army's tenets of operations; synchronization, integration, and depth. However, there is still much work to do in strengthening the Army's doctrinal understanding and explanation of CO.

Field Manual 3-38 as the Army's first doctrinal publication of its kind takes on the difficult task of introducing a new concept, CEMA. While introducing a new concept is difficult in any doctrinal endeavor, the added complexity of addressing actions that need to occur in a new

[127]Department of the Army, Field Manual 3-38, 1-5.

domain is immense. While the intent in raising cyber to a domain level was undoubtedly an effort to ensure adequate measures were being taken to address this new operational environment, it unintentionally created a mythical beast that knows no boundaries. The cyber beast has grown so large and complex that slaying or understanding it may seem unattainable. However, just as new theorists shout that their theory will provide all understanding and eliminate all friction, the hype eventually leads to a plateau. The cyber domain poses some unique challenges to the Army, but the acknowledgement of the complexity of the system of systems of cyberspace opens many possibilities to exploit and refine.

While the Army cannot lobby for revoking domain status from cyberspace it can strive to understand the doctrinal implications. Although, FM 3-38 continues to move the discourse along in understanding cyberspace, the placement of it in the Army's third tier of doctrinal hierarchy does not adequately institutionalize the importance of CO. Much of the difficulty in crafting cyber doctrine stems from the effects of adding cyber as a domain. The Army cannot change that fact; it can only move forward to prepare itself to face the threat and complexity of the modern operational environment.

However, the Army can elevate the placement of FM 3-38 to an Army Doctrinal Publication level. The ADPs provide the Army's fundamental principles and how those principles support ULO. "The purpose of FM 3-38 is to provide an overview of principles, tactics, and procedures of Army integration of CEMA as part of unified land operations."[128] FM 3-38 provides an overview of the principles of CEMA, but if CEMA is essential to conducting ULO its level of doctrinal importance moves from the tactical and procedural level of a field manual, towards the fundamental principles that support ULO as an ADP.[129]

---

[128]Ibid., v.

[129]Ibid., 1-3. Cyberspace operations, EW, and SMO are essential to the conduct of unified land operations.

While movement of the placement of FM 3-38 to an ADP may seem antidotal, it would also help strengthen the development of the concept of CEMA. As a new concept that integrates multiple types of operations, (CO, EW, and SMO), a field manual is hardly the place to expound upon a new concept that integrates multiple types of operations and defines relationships across the Army's theory of ULO. Although the term CEMA may not fully incorporate the entire spectrum of the global domain within the information environment of cyberspace, CEMA is now a fundamental principal within the Army and it will need to be integrated into all operations.

Moving CEMA up to the ADP level will enable supporting FMs and Army Techniques Publications to expand on the technology aspect of cyberspace. As a man-made domain, technological advancements will have a great impact with the governing tactics, techniques, and procedures. FMs and Army Techniques Publications could facilitate a partnership between some of the leading technological computing and software firms to maintain relevant FMs and Army Techniques Publications, as new technological advancements occur. The Army's doctrinal concept of 2015 supports this idea through the storage of Army Techniques Publications on a wiki type server.

The lack of a grand strategist in cyberspace most likely will prove irrelevant in cyber operations. The Army's theory of ULO has moved beyond any one theorist and as such, the integration of cyber operations is free to be developed and support ULO as part of the Army's system of war, instead of an unconnected component that some will claim overshadows all other forms of warfare. After all, Clausewitz states that "fighting is the central military act; all other activities merely support it."[130]

With the changes in perception of time and space in cyberspace, the Army's three tenets of synchronization, integration, and depth still hold valid in cyber operations. However, additions

[130]Clausewitz, 227.

to tactical terms are needed to further enhance the doctrinal development of CEMA and the desired effects that it can achieve. The Army's own lexicon of tactical tasks inhabits the assignment of tasks and purpose to cyber operations. Moving CEMA up to an ADP will give it the doctrinal framework structure necessary to influence changes in doctrinal lexicon.

As the cyber domain has changed the operational environment in which the Army operates, so must corresponding doctrine adjust in order to account for new opportunities for Army operations to exploit and achieve effects. The complexity of cyberspace creates opportunities. Although cyber operations may not cause defeat of an enemy by their operations alone, being combined, integrated, and synchronized across the full range of military operations provides another opportunity to gain a relative advantage.

BIBLIOGRAPHY

Ackerly, Bill. “Army's Top Signal Officer: Everything Is Network Dependent.” http://www.army.mil/article/82183/ (accessed February 20, 2014).

Air Force Basic Doctrine, Organization, and Command. *Air Force Doctrine Document 1*. Maxwell AFB, AL: United States Air Force, 14 October 2011.

Ancker III, COL(R) Clinton J., and LTC (R) Michael A. Scully. “Army Doctrine Publication 3-0: An Opportunity to Meet the Challenges of the Future.” *Military Review* (January-February 2013): 38-42.

Army Cyber Command/Fort Meade MD Army (2nd). *The US Army LandCyber White Paper 2018-2030*. Fort Meade, MD: US Army Cyber Command/2nd US Army, 9 September 2013.

Aucsmith, David. “A Theory of War in the Cyber Domain.” March 5, 2012. https://www.academia.edu/1753317/A_Theory_of_War_in_the_Cyber_Domain_An_Historical_Perspective (accessed December 26, 2013).

Campen, Alan D. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: AFCEA Internat Press, 1996.

Carr, Jeffrey. *Inside Cyber Warfare*. 2nd ed. Beijing: O’Reilly Media, 2012.

Cavelty, Myriam Dunn. “Unraveling the Stuxnet Effect: Of Much Persistence and Little Change in the Cyber Threats Debate.” *Military and Strategic Affairs* 3, no. 3 (December 2011): 11-20.

Clarke, Richard A., and Robert K. Knake. *Cyber War: the Next Threat to National Security and What to Do About It*. New York: Ecco, 2012.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Indexed Edition Reprint ed. Princeton, NJ: Princeton University Press, 1989.

Corbett, Sir Julian. *Some Principles of Maritime Strategy*. Annapolis, MD: United States Naval Institute, 1988.

Czosseck, Christian, and Kenneth Geers, eds. *The Virtual Battlefield: Perspectives On Cyber Warfare*. Vol. 3 of *Cryptology and Information Security Series*. The Netherlands: Ios Press, 2009.

Department of Defense. “Armed with Science.” The Official US Defense Department Science Blog. September 20, 2013. http://science.dodlive.mil/2013/09/20/untouchable-fighting-forward-in-the-space-cyber-domains/ (accessed March 17, 2014).

———. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, July 2011.

———. *Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations*, by Robert Gates. Washington, DC: Government Printing Office, June 23, 2009.

Department of Homeland Security. *The National Strategy to Secure Cyberspace*. Washington, DC: Government Printing Office, February 2003.

Department of the Army. Army Doctrine Publication 1, *The Army*. Change 1. Washington, DC: Headquarters, Department of Army, 7 November 2012.

———. Army Doctrine Publication 1-0, *Operational Terms and Military Symbols.* Washington, DC: Headquarters, Department of Army, August 2012.

———. Army Doctrine Publication 3-0, *Unified Land Operations*. Washington, DC: Headquarters, Department of Army, October 2011.

———. Army Doctrine Publication 3-05, *Special Operations*. Washington, DC: Headquarters, Department of Army, August 2012.

———. Army Doctrine Publication 5-0, *The Operation Process*. Washington, DC: Headquarters Department of the Army, 17 May 2012.

———. Army Doctrine Publication 6-0, *Mission Command*. Washington, DC: Headquarters, Department of Army, 10 September 2012.

———. Army Doctrine Reference Publication 1-02, *Operational Terms and Military Symbols.* Washington, DC: Headquarters, Department of Army, September 2012.

———. Army Doctrine Reference Publication 3-0, *Unified Land Operations*. Washington, DC: Headquarters Department of the Army, 16 May 2012.

———. Army Doctrine Reference Publication 3-90, *Offense and Defense*. Washington, DC: Headquarters Department of the Army, 31 August 2012.

———. Army Doctrine Reference Publication 5-0, *The Operation Process*. Washington, DC: Headquarters Department of the Army, 17 May 2012.

———. Field Manual (FM) 3-36, *Electronic Warfare*. Washington, DC: Headquarters Department of the Army, November 2012.

———. Field Manual 3-38, *Cyber Electromagnetic Activities*. Washington, DC: Headquarters Department of the Army, February 2014.

Deputy Directorate, Joint Staff, J-7, Joint Education and Doctrine, Joint Doctrine Analysis Division. *Compendium of Key Joint Doctrine Publications*. Washington, DC: Government Printing Office, 17 June 2013.

Dolman, Everett Carl. *Pure Strategy: Power and Principle in the Space and Information Age*. New York, NY: Routledge, 2005.

Drew, COL Dennis M., and Dr. Donald M. Snow. *Making Strategy: An Introduction to National Security and Process and Problems*. Maxwell Air Force Base, AL: Air University Press, August 1988.

Federal Communications Commission. Public Safety and Homeland Security Bureau. "Tech Topic 20: Cyber Security and Communications." http://transition.fcc.gov/pshs/techtopics/techtopics20.html (accessed March 17, 2014).

Gharajedaghi, Jamshid. *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*. 2nd ed. Boston, MA: Butterworth-Heinemann, 2006.

Harrison, Neil E., ed. *Complexity in World Politics: Concepts and Methods of a New Paradigm*. Suny Series in Global Politics. Albany: State University of New York Press, 2006.

Hayden, Gen Michael V. "The Future of Things 'Cyber'." *Strategic Studies Quarterly* (Spring 2011): 3-7. http://www.chertoffgroup.com/pdf/The-Future-of-Things-Cyber-by-Michael-Hayden-Strategic-Studies-Quarterly-Spring-2011.pdf (accessed January 30, 2014).

Intel Company. "Intel Facts." http://www.intel.com/content/www/us/en/company-overview/company-facts.html (accessed March 17, 2014).

Jackson, Aaron P. Dr. *The Roots of Military Doctrine: Change and Continuity in Understanding the Practice of Warfare*. Fort Leavenworth, KS: Combat Studies Institute Press, 2013.

Joint Chiefs of Staff. Joint Publication 1-0, *Doctrine for the Armed Forces of the United States*. Washington, DC: Joint Chief of Staff, March 2013.

———. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Joint Chief of Staff, September 2013.

———. Joint Publication 5-0, *Joint Operational Planning*. Washington, DC: Joint Chief of Staff, August 2011.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: Center for Technology and National Security Policy, 2009.

Libicki, Martin C. "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* (Fall 2012): 325-40. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf (accessed December 31, 2013).

———. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 23-39.

Maier, Mark W. "Architecting Principles for Systems-of-Systems." *Systems Engineering* 1, no. 4 (1998): 267-284.

Microsoft. "A History of Windows." http://windows.microsoft.com/is-IS/windows/history#T1=era5 (accessed March 17, 2014).

Mihalache, Adrian. “The Cyber Space-Time Continuum: Meaning and Metaphor.” *Information Society* 18, no. 4 (July 2002): 293-301.

Milevski, Lukas. “A Special Operation in Cyberspace?” *Joint Forces Quarterly* no. 63 (October 2011): 64-69.

———. “Strategy and Cyberpower: From Tactics to Politics.” *Infinity Journal* 3, no. 2 (Spring 2013). https://www.infinityjournal.com/article/96/Strategy_and_Cyberpower_From_Tactics_to_Politics/ (accessed December 26, 2013).

Naval Service. Naval Doctrinal Publication 1, *Naval Warfare*. United States Navy, 1 March 2010.

Rosenau, James N. “Thinking Theory Thoroughly.” In *The Scientific Study of Foreign Policy*, edited by James N. Rosenau, 19-31. London: Frances Pinter, 1980.

Ryan, Alex J. “What Is a Systems Approach?” http://arxiv.org/abs/0809.1698 (accessed April 1, 2014).

Schreier, Fred. “On Cyberwarfare.” *DCAF Horizon 2015 Working Paper* no. 7 (2012): 132.

Steed, Danny. “Cyber Power and Strategy-so What?” *Infinity Journal* 1, no. 2 (Spring 2011. https://www.infinityjournal.com/article/11/Cyber_Power_and_Strategy__So_What/ (accessed December 26, 2013).

The President of the United States. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Network World*. Washington, DC: The White House, May 2011.

US Air Force. Air Force Doctrine Document 1, *Air Force Basic Doctrine, Organization, and Command*. Maxwell AFB, AL: United States Air Force, 14 October 2011.

US Army Cyber Command. “Army Cyber.” http://www.arcyber.army.mil/org-arcyber.html (accessed March 19, 2014).

US Army Training and Doctrine Command. 2012 Army Posture Statement, “Doctrine 2015”. Posted February 12, 2012. https://secureweb2.hqda.pentagon.mil/vdas_army posturestatement/2012/InformationPapers/ViewPaper.aspx?id=322 (accessed November 23, 2013).

———. TRADOC Pamphlet 525-5-500, *The United States Army Commander’s Appreciation and Campaign Design Version 1.0.* Fort Monroe, VA: Department of the Army, 28 January 2008.

———. TRADOC Pamphlet 525-7-8, *The United States Army’s Cyberspace Operations Concept Capability Plan 2016-2028.* Fort Monroe, VA: Department of the Army, 22 February 2010.

US Strategic Command. “US Cyber Command.” http://www.stratcom.mil/factsheets/2/Cyber_Command/ (accessed January 23, 2014).

Wylie, J. C. *Military Strategy: A General Theory of Power Control*. New Brunswick, NJ: Rutgers University Press, 1967.