

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 20-04-2018		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) 25-07-2017 to 20-04-2018	
4. TITLE AND SUBTITLE Concepts for Conducting Warfare in Cyberspace			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Sean C. Heidergerken Lieutenant Colonel, United States Army			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton Blvd Norfolk, VA 23511-1702			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited					
13. SUPPLEMENTARY NOTES Not for commercial use without the express written permission of the author					
14. ABSTRACT <p>The recent elevation of cyberspace as a domain has been done without fully providing a theory of the strategic and operational construct of the implementation of cyber power. This has resulted in a focus on the tactical effects of cyber capabilities. This is not unlike the initial response following technological advancements in maritime power in the 19th century, and the advent of airpower in the early 20th century. For a state to wholly realize the full capabilities of cyberspace, as was accomplished in the maritime and air domains, strategic and operational planners require a construct upon which to base their planning efforts.</p> <p>By exploring the nature of the cyberspace domain alongside the initial theories of maritime and air power, this paper will offer a construct for planners and operational artists to take advantage of the benefits of the new domain. Current efforts have either focused on tactical effects or held cyber in reserve and protected for a future use. If the military is to take full advantage of the new domain, it must fully integrate effects from this synthetic domain in time and space with effects from the other physical domains to meet strategic goals.</p> <p>The operational construct presented is a four-layered concept of cyberspace that includes the physical, logic, data, and social layers. Despite a variety of possible actions against each of these layers, the operational tasks operational artists need to focus on are interdict, disrupt, corrupt, and destroy. By focusing on these key tasks, the operational artist is able will effectively integrate the effects from the cyberspace domain with effects from the physical domains for strategic effect.</p>					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Unclassified Unlimited	54	19b. TELEPHONE NUMBER (include area code)

THIS PAGE INTENTIONALLY LEFT BLANK

NATIONAL DEFENSE UNIVERSITY
JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL



CONCEPTS FOR CONDUCTING WARFARE IN CYBERSPACE

by

Sean C. Heidgerken

Lieutenant Colonel, United States Army

THIS PAGE INTENTIONALLY LEFT BLANK

CONCEPTS FOR CONDUCTING WARFARE IN CYBERSPACE

By

Sean C. Heidgerken

Lieutenant Colonel, United States Army


A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: 


20 April, 2018

Thesis Advisor:

Signature: 
Keith Dickson, Ph.D., Professor
Chair, Dept of History

Approved by:

Signature: 
James Fosbrink, Colonel, U.S. Army
Committee Member

Signature: 
Miguel L. Peko, Captain, US Navy
Director, Joint Advanced
Warfighting School

THIS PAGE INTENTIONALLY LEFT BLANK

Abstract

The recent elevation of cyberspace as a domain has occurred without fully providing a theory of the strategic and operational construct of the implementation of cyber power. This has resulted in a focus on the tactical effects of cyber capabilities. This is not unlike the initial response following technological advancements in maritime power in the 19th century, and the advent of airpower in the early 20th century. For a state to wholly realize the full capabilities of cyberspace, as was accomplished in the maritime and air domains, strategic and operational planners require a construct upon which to base their planning efforts.

By exploring the nature of the cyberspace domain alongside the initial theories of maritime and air power, this paper will offer a construct for planners and operational artists to take advantage of the benefits of the new domain. Current efforts have either focused on tactical effects or held cyber in reserve and protected for a future use. If the military is to take full advantage of the new domain, it must fully integrate effects from this synthetic domain in time and space with effects from the other physical domains to meet strategic goals.

The operational construct presented is a four-layered concept of cyberspace that includes the physical, logic, data, and social layers. Despite a variety of possible actions against each of these layers, the operational tasks that operational artists need to focus on are interdict, disrupt, corrupt, and destroy. By focusing on these key tasks, the operational artist will effectively integrate the effects from the cyberspace domain with effects from the physical domains for strategic effect.

Dedication

Dedicated to my wife and daughters who have been a constant source of support and encouragement during the multiple deployments and understanding of the time devoted to this work. I am truly thankful to have you in my life.

Acknowledgments

I would like to thank Dr. Keith Dickson for his guidance and mentorship. His ability to guide me through the development of the ideas contained in this work have been invaluable. His insights have greatly elevated the quality of both my learning process and this paper.

I am also deeply appreciative of the insights and efforts of Colonel Jorge Cordeiro that have resulted in a more focused paper.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Abstract	iii
Dedication	iv
Acknowledgments	v
CHAPTER 1: DEFINING THE NEED FOR CYBER POWER THEORY	1
What is the cyberspace domain?	3
Why is Theory Important?	5
Research Approach	5
CHAPTER 2: AN EXPLORATION OF CYBERSPACE: WHAT IS THE NATURE OF THE DOMAIN?	7
Cyberspace Domain	7
The Four Layers of the Cyberspace Domain	9
Warfare and Cyberspace	10
CHAPTER 3: SEA POWER EMPLOYED WITHIN ITS DOMAIN: APPLICATIONS FOR THE CYBER DOMAIN	14
Geographic Determinants	14
Character Aspects	16

CHAPTER 4: AIR POWER EMPLOYED WITHIN ITS DOMAIN: A CONCEPTUAL MODEL FOR CYBER POWER	19
New Domain Power and Future War.....	19
Airpower and Cyber Power	24
CHAPTER 5: A CONCEPTUAL MODEL FOR CYBERSPACE OPERATIONS	26
The Choice to Use Cyberspace.....	26
Time and Space Effects of Cyber Operations.....	27
Targeting Intimacy.....	28
Advantage of Proximity	30
Key Concepts	31
CHAPTER 6: AN OPERATIONAL CONCEPT FOR CYBERPOWER	32
Cyberspace Lessons from Early Maritime and Air Theorists.....	32
Operational Concepts.....	34
Conclusion	36
BIBLIOGRAPHY.....	38
VITA.....	42

CHAPTER 1: DEFINING THE NEED FOR CYBER POWER THEORY

Aeronautics opened up to men a new field of action, the field of the air. In doing so, it of necessity created a new battlefield; for wherever two men meet, conflict is inevitable. - Douhet¹

In the opening lines of his treatise on air power the Italian theorist, Giulio Douhet, could just as easily have been describing cyberspace as a new field of action and a new battlefield. Cyberspace has the potential to change war in a way not experienced in 100 years.² There exists a general belief that cyberspace is useful in the conduct of current and future warfare, however, a clear conceptual basis for the operational or strategic employment of this emerging form of power is lacking. By reviewing the work of theorists who adapted technological advances in the maritime and air domains to a strategic use, this paper will take the same approach for cyberspace. An examination of early cyberspace operations will highlight key concepts necessary to apply cyber power at the strategic and operational levels of war.

Although, the advent of a new domain does not change the nature of war, it does allow for the application of military power in new ways and thus changes the character of war. Governments are already employing cyberspace as a warfighting domain. For example, the United States is in the process of elevating the United States' Cyber Command (USCYBERCOM) to combatant command (CCMD) status, centralizing the

¹ Giulio Douhet, *Command of the Air* (North Stratford, NH: Ayer Company, 1942), 3.

² *DOD Dictionary of Military and Associated Terms*. (Washington, D.C.: Dept. of Defense, 2017). Defines cyberspace as, "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

command and control of DoD offensive and defensive cyber operations under one command.³ Kenneth P. Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security, stated that the US is resolved to "embrace the changing nature of warfare and maintain U.S. military superiority across all domains and phases of conflict."⁴ Other nations, including Russia, China, the United Kingdom, France, and Israel, have established similar organizations. Non-state actors, such as the Islamic State and al Qaida, have used cyberspace as a warfighting domain. Still other non-governmental groups, such as the Anonymous "hacker collective," have come into existence for the sole purpose of exploiting cyberspace for disruptive purposes.

The challenge for any military (or quasi-military) organization attempting to gain an advantage from a new technology is the need to employ it operationally. For a new domain to be operationally useful, a clear understanding of its nature is required, as well as a clear grasp of certain principals of operation. These intellectual constructs lead to the development of a theoretical construct to support operational warfighting. Without a theoretical base, operational leaders and planners risk misapplying or ignoring capabilities through ignorance of the military applications of cyberspace.

US military thinking about cyberspace has largely focused on tactical applications. This is because there has been little thinking directed to the development of a military cyber power theory that leads the operational artist to incorporate cyber technology effectively within the operational factors of time, space, and forces to achieve

³ Jim Garamone and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," DoD News, Defense News Agency, August 18, 2017.

⁴ Garamone and Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command."

a strategic effect. Such a theory also provides national level leaders strategic-operational rational building long-term capabilities.

A similar requirement for an operational warfighting theory existed for the development of the maritime and air domains in the nineteenth and twentieth centuries. Theorists such as Alfred Thayer Mahan and Julian S. Corbett established the conceptual theory for maritime power. Giulio Douhet and William Mitchell did the same for airpower, and laid the groundwork that enabled operational and strategic planners to take full advantage of the military applications for each domain. The same requirement now exists as cyberspace emerges as a significant warfighting domain.

What is the cyberspace domain?

Cyberspace interacts differently with the other warfighting domains than they do with each other. It relies on the other domains for its physical nature and exists only in conjunction with one or more physical domains. U.S. military thinking recognizes five operational domains: land, maritime, air, space, and cyberspace. Dividing the battlespace into domains serves to provide a framework to deliver effects. The land, maritime, air, and space domains are physical and understood as part of the natural universe.

Cyberspace as a domain is conceptually more complicated because it has physical, synthetic, and virtual characteristics. It therefore requires a unique approach to gain understanding. Actions initiated in a virtual domain have different outcomes than in the physical domains; likewise, as a synthetic, or man-made, domain, cyberspace presents infinite capabilities not altogether subject to control. Although cyberspace infrastructure exists in the physical world and requires physical elements for its existence, cyberspace pervades all other domains, and in specific instances, can dominate other domains in

ways that a physical domain cannot.

Describing cyberspace itself and the instruments that are essential to the domain often causes confusion due to limited ability of current language terms to describe it. Some have attempted draw parallels to the natural domains to describe aspects of cyberspace. These efforts, however, often fall short. For example, “cyber” is used both as a descriptor (as in “cyberspace domain”) and as a capability (as in “cyber weapons”). This disjointed nature of describing cyberspace is not unusual. This use of conflicting terms to describe aspects of a new domain occurred in early descriptions of the air domain when vehicles that took to the skies were originally referred to as airships, borrowing a term from the maritime domain. Cyber-specific words may develop as the domain evolves, expands, and matures.⁵

The DoD defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”⁶ This definition highlights the technological aspect of the domain and implies that it is nothing more than an impersonal machine-based system. This definition does not capture the synthetic and dynamic aspects of the domain, nor, provides an appreciation for the importance of human interaction.

The DoD does not have a definition of cyber power or cyber war. National Defense University’s Daniel Kuehl has defined cyber power as “the ability to use

⁵ Where the Department of Defense (DoD) has a definition of a term it will be used as the standard unless otherwise noted. However, there are a number of terms that the DoD has yet to provide definitions to. In these cases, the definitions provided by other cyber writers will be used.

⁶ Headquarters, Joint Staff. (2013). Cyberspace Operations (JP 3-12(R)), GL-4.

cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.”⁷ Richard Clarke, an early cyber power theorist provides a definition of cyber war as the “actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption.”⁸ These definitions will serve to support an analytical model that will guide the development of a military cyber power theory.

Why is Theory Important?

As was the case in the maritime and air domains, it is important to develop a sound theoretical concept for the cyberspace domain to gain strategic and operational advantage in war. The theoretical concept provides the intellectual underpinnings necessary for any significant application of cyber power in waging war as well as having an appreciation of cyberspace as a warfighting domain. There is value in the intellectual process of assessing, evaluating, examining, understanding, and developing warfighting concepts.

Research Approach

This paper will address the need for a cyber operational construct by examining the writings of A.T. Mahan and Giulio Douhet to develop a description of the nature and principles of the cyber domain. Just as Mahan and Douhet addressed these questions for their operational domains, their analytical approach will serve as a model for developing an initial theory for applying cyber capabilities in support of operational warfighting will be presented.

⁷ Larry K. Wentz, Starr H. Stuart, and Kramer D. Franklin, *Cyberpower and National Security* (Washington, D C: Potomac Books, 2009), 35.

⁸ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2010), 6.

The paper will offer a description of cyberspace, its attributes, and a simple description of warfare in the domain, while referencing the other physical domains. An exploration of both Department of Defense doctrine and the writings of a number of cyber theorists will establish a basic understanding of the domain. A.T. Mahan's six determinants of sea power is applied to the development of cyber power, as is the application of lessons from air power theorist Giulio Douhet by applying two assumptions and five characteristics to cyber power. Deriving lessons from early cyber operations will assist in presenting the theoretical concept.

CHAPTER 2: AN EXPLORATION OF CYBERSPACE: WHAT IS THE NATURE OF THE DOMAIN?

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system.

Unthinkable complexity.

— William Gibson, *Neuromancer*

The science fiction writer William Gibson coined the term cyberspace in the early 1980s to describe networked communication between computers. Today, cyberspace is a term used to describe the system of all the world's computer networks and their connections.¹ Since the early electronic communications systems of the nineteenth century, the interconnectedness of both humans and machines has grown exponentially to the point where cyberspace is inseparable from human interactions in the twenty-first century.² States must now take into account how they will use cyberspace to gain advantage over adversaries. To begin the exploration of this requirement, this chapter will define the cyberspace domain, describe its layered characteristics, and begin the discussion of warfare and operations in the domain.

Cyberspace Domain

As noted previously, cyberspace has physical, synthetic, and virtual characteristics. A widespread misconception within military thinking is that cyberspace is simply the digital machines and the communications between them. All of cyberspace exists on electronic machinery that resides in the physical world. A typical example is the

¹ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2010), 70.

² Some scholars trace the internet back to the advent of the telegraph because it is the first electronic form of communication. Much of the current digital infrastructure follows the same infrastructure pathways first established to carry telegraph signals.

definition of cyberspace in Joint Publication 3.12, Cyber Operations, which describes cyber operations as “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”³ In this way, it is possible to destroy the data in cyberspace by destroying the machine on which it resides. This appears to be a definition for a future capability. The problem is that no one has effectively expressed how to achieve objectives in and through cyberspace including offensive, defensive and information network operations. This view of cyberspace is too simplistic for any operational application. A more sophisticated approach involves understanding the ubiquitous nature of cyberspace, its connection to all other domains, the reliance of modern society on its existence, and its ability to influence human behavior.

Cyberspace exists simultaneously within and apart from the other domains.⁴ In the simplest terms, as the DoD definition implies, cyberspace is the digital machines and the communications architecture between them. This means that all of the information that gives the cyberspace its virtual aspect resides on a piece of physical hardware existing somewhere in one or more of the other domains.

The essential nature of cyberspace is continuous change. As new technology is developed and integrated into cyberspace, the physical structures and means of communication change as well. Cyberspace is in a continuous process of construction and destruction, and renewing itself in nearly infinite variety.

Because cyberspace is man-made, artificial, and unlike other domains, it may be

³ Headquarters, Joint Staff. (2013). Cyberspace Operations (JP 3-12(R)), II-1.

⁴ Larry D. Welch, "Cyberspace - the Fifth Operational Domain." *Institute for Defense Analyses Research Notes Summer 2011*: October 28, 2017: 3.

shaped, manipulated, or destroyed to serve an intended purpose. Further, because it is virtual, humans cannot physically enter cyberspace. To have effects on human behavior and will, actions initiated within cyberspace only have observable effects outside of the domain itself. To take full advantage of the unique nature of cyberspace, it is essential to understand the conditions and characteristics of the domain. To begin, a description of cyberspace is that it is a system consisting of numerous layers.

The Four Layers of the Cyberspace Domain

The cyberspace theorist Alexander Klimburg has proposed a model of cyberspace as a system consisting of four layers that effectively accounts for the interaction of actual humans in the domain.⁵ The first layer is the physical, consisting of the hardware, the computers, cables, and communications equipment that makes up the cyberspace.⁶ Humans work, input, or retrieve all of the information residing in this layer. Klimburg describes the physical layer as the bones of cyberspace.⁷

The second layer, the logic layer, is where the coded software and protocols reside. Code represents the laws that govern what the physical layer does. The laws that govern the cyberspace domain are different from the laws that govern of the physical domains in that they are human creations and therefore, alterable. Klimburg relates this

⁵ Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin Press, 2017), 28-51. In Joint Publication 3.12, the DoD describes cyberspace as being comprised of three layers: physical network, logical network, and cyber-persona. The physical layer consists of the physical networks that transmit data. This layer is the location where the elements of the networks exist in the other four domains. The logical layer represents the interconnected vital networks abstracted from the physical network. In this layer, code can exist in multiple locations in the physical layer, but be accessed by a single address. The cyber-persona layer is further abstracted and is the virtual representation of persons or entities on the network. One individual can have multiple persona. Though this model accounts for human interaction in the domain, it does not account for the actual humans that interact and ultimately are the purpose for cyberspace.

⁶ Klimburg, 28-34.

⁷ Ibid., 28

layer to the body's central nervous system because it "powers all the functions of the physical layer and enables information to travel over it."⁸ The need for systems to communicate has resulted in standards that allow data to move from one area of cyberspace to another. For example, a "domain network system" routes information across a web-like communications structure using a set of designed standards to allow data to move from a sender to an intended receiver.

The third layer is the data layer, containing all of the information uploaded through human communications as well as all the information resulting from machine-to-machine communications. Klimburg equates this layer to the muscular system.⁹ Just as humans have different types of muscles, cyberspace contains different types of data. Ease of retrieval characterizes one type of data while other data resides, more or less, invisible to common users and allows the system to function automatically.

The forth layer is the social layer. Klimburg refers to this layer as the "human actions and aspirations that make the internet and cyberspace what they are."¹⁰ Human involvement and interface is the essential aspect of the cyberspace domain, or the making of judgements and realization of cognitive effects.¹¹ Because altering human behavior through decision-making is ultimately the purpose of all military cyber operations, this layer is the ultimate target for operations in cyberspace.

Warfare and Cyberspace

A useful definition of cyber warfare is "the set of all lethal and non-lethal

⁸ Ibid., 35.

⁹ Ibid., 40.

¹⁰ Ibid., 29.

¹¹ Ibid., 50.

activities undertaken to subdue the hostile will of an adversary or enemy.”¹² Although, warfare in cyberspace is unique, it is no more unique than the distinctions between warfare on land, sea, air, or in space.¹³ Cyberspace is unique because the intended effects occur not within the domain, but throughout the other physical domains according to an operational intent.

An example of the use of cyber space comes from General Raymond A. Thomas III, the commander of US Special Operations Command, who reported in December of 2017 that US forces employed “combined offensive cyber operations with information operations, financial disruption, and kinetic effects to destroy an adversary on an epic scale”.¹⁴ Here is the first inkling of an appreciation for cyberspace as an operational tool. Although lacking detailed descriptions of the cyber operation, the linking of the act to other domains makes this significant. However, the tactical focus of the mission demonstrates a lack of an appreciation of the possibility of neutralizing an enemy at the strategic-operational level in such a way that all other capabilities in other domains can easily dominate and compel.

If an enemy is reliant to some degree on cyber power for its military or political effectiveness, cyber power properly applied will contribute to the destruction of enemy forces. The combination of cyber power with other actions such as information operation, financial disruption, and/or conventional firepower will amplify the effectiveness of military operations. For this reason, it is important for the operational artist to understand

¹² Clarke and Knake, 232.

¹³ Brett T. Williams, "Ten Propositions Regarding Cyber Operations." *JFQ: Joint Force Quarterly*, no. 61 (2d Quarter 2011):11.

¹⁴ David Vergun, “Commanders Need Latitude to Employ Offensive Cyber, Says GEN Thomas,” *Army News Service*, December 12, 2017.

cyber power in an operational context.

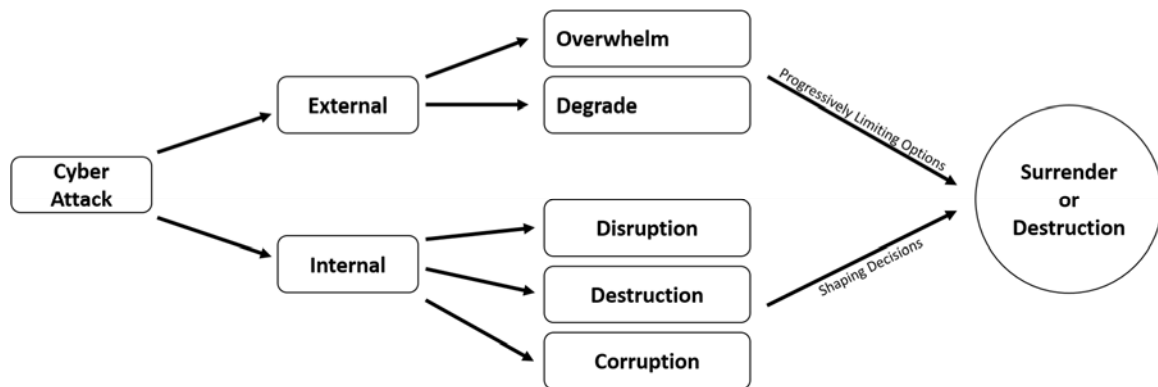


Figure 1 Decomposition a Cyber Attack

Martin Libicki defines a cyberattack, or “offensive cyber operations,” as a digital based operation calculated to affect an information system’s ability to produce reliable information or cause it to produce bad decisions.¹⁵ Cyberattacks can have a variety of effects, such as disruption, corruption, and possibly the destruction of the system, or the machines themselves (see figure 1). Disruption is tricking a system to shut down, slow down or perform in a degraded capacity. Corruption is the altering of code to change its function within a system. Disruption and corruption are similar in the effect, but disruption tends to be more obvious, whereas corruption is more subtle and perhaps latent. Destruction is causing a system to operate in a manner that key parts (including machines) perform outside their intended parameters and become non-functioning. Describing cyberattacks as internal or external or external is useful. An internal attack occurs within the targeted system. External attacks target the communications networks by either overwhelming the system so no traffic can pass through, or by redirecting traffic to another unintended location.¹⁶ Though this definition focuses on cyber-attack alone,

¹⁵ Martin Libicki, *Cyberspace in Peace and War*, Annapolis, (MD: Naval Institute Press, 2016), 19.

¹⁶ Libicki, 19. Disruption attacks “trick” systems into performing incorrect operations that: shut them down, work at reduced capability, force obvious errors, or interfere with the operation of other systems.

the operational artist needs to understand that these types of attacks require integration with other capabilities to have maximum strategic-operational effect.

The more significant challenge in cyberspace is in the defense. In the physical domains, location limits the avenues of attack of the two opposing forces and regardless of the technologies available to them. The very nature of the global network and its web-like construction results in near infinite avenues of approach for a potential attacker to use.¹⁷ This includes both government and commercial systems. The operational planner must ensure defensive actions are integrated with other capabilities despite their dominance in cyber operations.

Having presented the nature of cyberspace in simplified language, the following two chapters will offer examples of principles of operation based on the conceptual theories of the maritime and air domains. Mahan offers a theory of the reconceptualization of the maritime domain's strategic and operational purpose by taking advantage of technology. On the other hand, Douhet provides insights into the changes of strategic-operational application of military force due to the emergence of a new domain. As in these domains, cyberspace must become a domain in which that the operational artist is fully cognizant of and completely confident in employing power.

Corruption attacks change data or algorithmic functions in unauthorized ways. To distinguish between these two forms of attacks, Libicki offers the rule of thumb that corruption attacks are usually immediately obvious and extreme. On the other hand, corruption attacks are more subtle, difficult to detect, and have lingering, hard to diagnose causes. Destruction attacks, though rare are attacks where machines are given instructions that physically destroy the machine.

¹⁷ Ibid, 21.

CHAPTER 3: SEA POWER EMPLOYED WITHIN ITS DOMAIN: APPLICATIONS FOR THE CYBER DOMAIN

Among all changes, the nature of man remains much the same; the personal equation, though uncertain in quantity and quality in the particular instance, is sure to be found –
*A.T. Mahan*¹

Alfred Thayer Mahan's *Influence of Sea Power Upon History* was written at a time when technology was changing the character of warfare in a warfighting domain.

Mahan outlined six determinates of maritime power that also have correlates to the cyberspace domain: geographic position, physical conformation, extent of territory, number of population, character of the people, and the character of the government.²

Mahan's determinates offer a framework to explore the strategic and operational advantage achievable by exploiting emerging technology within a domain. In Mahan's theory, the ability of a state to become a sea power was a function of certain geographic aspects combined with the nature of the society and the state. Cyber power relies on similar concepts. Unlike the sea domain, the synthetic nature of the structure of cyberspace places no geographic constraints on any state (or non-state). Likewise, the physical and societal aspects related to the cyber domain have similar parallels to Mahan's concepts of the domain.

Geographic Determinants

Mahan's emphasis on a state's ability to operate in the sea domain is a matter of configuration of physical space. Thus, geographic conditions must be conducive to the states interests in operating in this domain. For a sea power, this means accessible coastlines and good harbors.³

¹ A.T. Mahan, *The Influence of Sea Power upon History, 1660-1783* (Mineola, NY: Dover, 1987) 89.

² Mahan, 28.

³ Ibid, 35, 43.

Configuration of physical space also influences how cyber power is used. Quite simply, states that control access to cyberspace will have a marked advantage over those who rely on others for their access. The location is no longer physical geographical access to the domain; for the cyber domain, access relates to the location of the physical layer of cyberspace. If a state controls the physical systems of cyberspace, it gains an advantage of access. Like the sea, cyberspace also has areas through which the bulk of the communications flows, known as Tier 1 Internet Service Providers. Until recently, the bulk of these providers were located in the U.S. and as a result, the vast majority of internet traffic has flowed through a U.S. owned, and consequently controlled, infrastructure.⁴ From an operational warfighting perspective, the U.S. has the initial advantage in cyberspace, as it controls access. Although this has begun to change in recent years, the fact remains that the states that control the access to cyberspace will have a significant advantage over those states who do not control access.

States are no longer reliant on the natural formations determining their access to global commons and more specifically to trade. Because the nature of cyberspace is synthetic, any state with the proper investment can build the architecture to gain access to cyberspace and have a degree of control. Estonia was vulnerable to Russian cyber-attack in 2007, leading it to move in a Mahanian direction to limit vulnerabilities by creating its own access to the cyber domain. Today, Estonia has become a leader of cyber operations within NATO to the level that it is the location of the alliance's Cyber Center of Excellence; primarily because it built the architecture to gain a greater degree of access than other states. As one of the most connected nations in Europe, it is the logical choice

⁴ Kris E. Barcomb, "From Sea Power to Cyber Power," *Joint Force Quarterly*, no. 69 (2nd Quarter 2013), 81.

for such an organization. As Estonia demonstrates, design of the networks and their connection to other portions of cyberspace, not geographic formations, is the basis of power within cyberspace.

In the development of cyber power, a state must ensure it has both cyber access, and high quality access. The U.S. has been the leading developer of the cyberspace domain to this point, but it does not currently have the highest quality. The sheer size of its information infrastructure offsets the lack of high quality. South Korea and Estonia have both significantly invested in improving access to the point that they lead the world in access quality.

Character Aspects

The second of the three determinants in Mahan's theory of sea power is concerned with the characteristics of the people and their government. Mahan proposed that for a state to become a maritime power, it needed a population that was willing to engage in the domain primarily for commercial benefit, which would lead the government also to engage in the domain to protect its economic interests.⁵ Mahan pointed out that in the sea domain, a state's total population was less important than the proportion of that population connected to the sea domain. Thus, a small state could become a major naval power through the connection of a majority of its population the sea domain.⁶

Just as in the sea domain, in the cyber domain it remains significant that it is not the total size of the population, but the number of the citizens who can navigate cyberspace as skilled experts rather than just consumers, which is important to becoming

⁵ Mahan, 44.

⁶ Ibid, 45, 50.

a power in cyberspace. States that desire to be cyber powers will need to promote specialization within its population to support and expand cyberspace capabilities as a means of gaining economic advantages, but also to protect and secure access to the cyber domain.

The commercial advantages of operating in the cyber domain are similar to those of the sea domain. The growth of internet commerce is a global phenomenon and now nearly indispensable. For a state to be a long-term cyber power, in the same way a state became a naval power, it will need to advance the commercial development of cyberspace. The synthetic nature of cyberspace differs from the maritime domain in so much, that commerce actually causes cyberspace to grow, whereas the maritime domain as a physical domain cannot change. This means that the state that leads the commercial development of cyberspace, actually, will have a direct effect on the size and character of the domain itself. Because the domain has the ability for unlimited expansion, no state can gain complete dominance.

Governmental support to free and open cyber commerce has benefited all states, but such freedom requires a commitment from government to protect these commercial pathways, just as Mahan observed in the sea domain. This means that states will need to have strong defenses to maintain the commerce in cyberspace, as they needed navies to protect commerce on the high seas. It is reasonable that governments set policies for the training and education of its citizens that encourage them to engage in cyberspace and enhance the development of cyber power. This government initiative replicates the same process that emerging maritime states used to create sea power and that was advocated so strongly by Mahan. It is reasonable; therefore, that the policies governments set regarding

the training and education of its citizens to be encouraged to engage in cyberspace as they did regarding the sea will also contribute to the development of cyber power. Quasi-authoritarian states like Russia and China are already developing cyber experts to serve the interests of the state, though, it is not clear these efforts will outpace free market states.

The basic threads Mahan lays out in describing the importance of a government's character in the development of maritime power have a direct correlation to the development of cyber power. In both the sea domain and the cyber domain, the governments that sponsor growth within the domain will determine the course of its development and reap the benefits. From an operational warfighting perspective, those states that control the infrastructure that makes up the physical nature of the domain will continue to exercise more influence than states that rely on the infrastructure of others for access.

CHAPTER 4: AIR POWER EMPLOYED WITHIN ITS DOMAIN: A CONCEPTUAL MODEL FOR CYBER POWER

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after changes occur. - Douhet¹

Guilio Douhet wrote *The Command of the Air* following the end of World War I.

Douhet's writings examine the strategic-operational effects of new technology on war.

Though often compared to Mahan, Douhet was more audacious and assertive in his views and recommendations for air power than Mahan's more carefully constructed historical analysis. Mahan believed that the principles of war do not change, only the methods.

Douhet took the opposite view, asserting that because the methods of war were changing, the very nature of war was also changing.² He saw air power as the key to -future war concept because of the uniqueness and overwhelming capabilities air power represented.

There are those who claim the emergence of cyber power is having the same effect today.

There is value in exploring Douhet's predictions of how air power would shape future war to seek insights on operations in the cyber operational domain.³

New Domain Power and Future War

Douhet postulated air power would be decisive in future war. Because ground and sea forces could not provide "effective defense against determined efforts of the enemy," when the enemy attacked the defenseless interior of a state via air power.⁴ By decisive, he proffered that the state with the most effective air force would have the advantage

¹ Douhet, 30.

² Benard Brodie, *The Heritage of Douhet*, (Santa Monica, CA : Rand, 1952), 4-5.

³ This concept is adopted from the World War II Era air power theorist Edward Warner's 1943 essay on early air power theorists published in the first edition of *Makers of Modern Strategy*.

Edward Warner, "Chapter 20: Douhet, Mitchell, Seversky: Theories of Air Warfare," in *Makers of Modern Strategy: Military Thought from Machiavelli*, Ed. Edward Mead Earle (Princeton: Princeton University Press, 1948), 489.

⁴ Mahan, 10.

in war by combining air power with the land and sea forces responsible for defending the homeland.⁵ Though air power never fully became the decisive operational power Douhet foresaw, modern warfare requires the employment of air power in combined arms maneuver to successfully achieve strategic-operational objectives.

The offensive nature of cyber power lends itself to similar claims of it being decisive in future war. Few if any cyber theorists make the claim that the effects of cyber-attacks will be the decisive action in a conflict. Rather they agree that strategic-operational cyber operations will be most effective when combined with operations in the physical operational domains. This precept highlights that the most effective military operations will integrate actions and effects from all the operational domains.

Douhet believed in the invulnerability of air power because he saw no effective way for a state to provide a defense against it. He envisioned a time when only aircraft would be capable of offensive maneuver due to their speed and lack of any countermeasures.⁶ The range and maneuverability of aircraft afforded advantage to the state with the best air force because the defender would then need to defend everywhere at all times.⁷ He did not believe that air defense weapons would be able to defend large parts of territory without focusing significant resources to just this aspect of defense.

Douhet further claimed that “to assure an adequate national defense, it is necessary and sufficient to be in a position in case of war to conquer the command of the air.”⁸ Douhet defines command of the air as to ability to be able to prevent the

⁵ Douhet, 253.

⁶ Ibid, 16.

⁷ Ibid, 10.

⁸ Ibid, 28.

enemy from flying while maintaining one's own capability.⁹ Without total control of the air, a nation would always be in danger of attack by the enemy. Douhet summarized the primacy of air power as, "to have command of the air is to have *victory*. Without this command, one's portion is defeat."¹⁰ Airpower would be decisive, it will be largely invulnerable, and it will target military, civilian, and government targets throughout the battlespace. Thus, shock and overwhelming power will characterize air as a warfighting domain. Other domains will shrink to insignificance in future war.

On examining Douhet's ideas, the cyber domain holds the potential for similar effects against military, civilian, and governmental targets. Like Douhet in 1923, the potential exists for cyber as a warfighting domain, like air, to be decisive. The enticing question is how can the cyber domain be elevated to this level? Much like Douhet's conceptualization of air as a warfighting domain, cyber consists of a unique and overwhelming capability.

Cyber offers a similar promise of fighting without concern for national borders. Whereas all with eyes and ears can see an air attack, only those appropriately actively watching know if a cyberattack is underway. The low cost of achieving a cyber offensive capability further complicates concerns and means anyone with a minimal amount of skill can be a potential attacker. These two aspects require cooperation between governmental security forces as well as the private sector.

Douhet predicted a time when air power would grow beyond mere support to ground forces and air-to-air combat. He saw that the true power of the air domain was in the ability to deliver both physical and psychological effects; to not only military targets,

⁹ Ibid, 24.

¹⁰ Ibid, 25, Italics are the author's.

but also to governmental, industrial, and civilian targets. Douhet stressed that the objective of aerial attack is the industrial and population centers located away from the surface forces.¹¹ The intent of these attacks was to “demolish the target, set it on fire and prevent fire fighters from extinguishing the fires.”¹² This new form of deep battle now could influence national level decision makers both where they lived and worked as well as their constituents. In this way, the societal impact of war would be increased and less restricted to the military and the front lines.

Application of the precept of targeting government, industry and the population is readily transferable to the cyberspace domain. Cyber operations originated in the civilian section and were adapted to military uses later. This is the reverse of the application of air power. The Russian attack on Ukraine is an example of the military application of cyber power targeting non-military targets on a limited scale. This and other limited uses of cyber power provide insight into the potential use in a large-scale war. The ever-increasing levels of automation means that the operational planner employing cyber power will possibly need to develop the means to conduct unrestricted war to preserve the state from within cyberspace.

Air power’s ability to destroy the enemy’s capability to wage war and undermine the populations will therefore influence decision makers.¹³ By targeting not only the military apparatus of a state but also its moral through deep attacks, Douhet felt that the character of the air domain was one of shock and overwhelming power where civilian morale and resistance would be shattered by air bombardment of population

¹¹ Ibid, 20.

¹² Ibid, 20.

¹³ Warner, 490.

centers.¹⁴ The physical and psychological targeting of civilian infrastructure and populations to yield a decisive effect on its own are also key tenets of cyber warfare advocates. Douhetian scenarios of societal and governmental collapse following a cyber-attack on a nation's power infrastructure are ubiquitous. The Russian cyber-attack against Ukraine in 2015 demonstrates the potential of psychological targeting effects on a population.¹⁵

The connected nature of communications in the world and the ability to propagate information and misinformation as well as the ability to affect directly modern conveniences using cyber resources affords strategic-operational planners unprecedented access to adversary populations. This access if properly planned for and executed, can have the overwhelming effect on the popular will that Douhet envisioned occurring with strategic bombing. Comprehensive access to both military and civilian adversary capabilities creates opportunities to influence decision makers both during declared hostilities and open conflict that can influence the population's will, and therefore influencing decision makers' actions.

For the reasons outlined above and because he saw air power as more economical, Douhet predicted that air power would become the dominant form of warfare in future war. Though he did not advocate for the total dismissal of land and sea forces, he believed that air power would be the most effective military arm.¹⁶ Air forces would be the single decisive element and the air domain would therefore become the only relevant strategic-operational warfighting domain. Land and sea

¹⁴ Mahan, 50.

¹⁵ Klimburg, 220.

¹⁶ Douhet, 188.

forces would fulfill largely defensive roles in support of the homeland.¹⁷ The purpose of these forces is to hold a front and to prevent an enemy's seizure of key terrain or industries. Douhet further states that defensive lines actually offer no protection from the air and that objectives are vulnerable. In short, the land and maritime domains would shrink in significance in future war when compared to the air domain.

Outside of science fiction there are few serious theorists advocating a position that cyber will ever become the most dominant domain in warfare. Cyber power, however, possesses the potential to become an increasingly important aspect of combined arms maneuver due to its economy and ability to transcend physical borders.

Airpower and Cyber Power

Douhet's concepts are useful in the development of theories and employment of strategic and operational cyber power. Unlike early air power advocates, no one currently proposes that cyber warfare will supplant all other forms of conflict. It remains important to ensure that cyberspace theories are further developed and that they incorporate multi-domain concepts. Actions in all the domains are only effective when coordinated.

Though both air and cyber power actions can be decisive, their employment in and of themselves will not be singularly decisive. The unique and potentially overwhelming aspects of cyber power will only reach their full potential when integrated into multi-domain combined arms maneuver. Though cyber power is unpopular in some circles, it is for reasons outside of Douhet's proposals outlined in 1923 regarding air power.¹⁸ In the case of cyber power, the reluctance to employ it for strategic-operational effect is due to misunderstandings on how to properly use the cyber domain to gain

¹⁷ Ibid, 175.

¹⁸ Douhet 255

advantage.

The final lesson learned from Douhet's work is his example of intellectual engagement to apply technology in a new domain for strategic and operational purposes. Though he was not correct in all of his predictions, his approach remains valid in the development of similar concepts for cyberspace. The next chapter will explore a template for the strategic and operational employment of cyber power.

CHAPTER 5: A CONCEPTUAL MODEL FOR CYBERSPACE OPERATIONS

The art of aerial warfare is not yet standardized, like the art of land and sea warfare, and there is still room for ingenuity. - Douhet¹

Cyberspace, as the first synthetic operational domain, has the potential to change the character of war in ways not yet understood or appreciated. To take full military advantage of this domain, a number of precepts need to be developed and articulated to provide a strategic and operational framework for an operational concept for the employment of cyber power. “Strategic and operational planners must focus on the significant and important precept of deliberate and conscious use of cyber space for achieving their effects or objectives.. Additionally, cyberspace has the ability to create operational space and time in the other domains. To achieve advantage in cyberspace, planners must also understand both the required target intimacy and proximity factors in order to take full advantage of the domain.

The Choice to Use Cyberspace

Because of its synthetic nature, cyberspace is the only domain that presents an option as to whether it has operational utility. It is the domain of choice. Another way to explain the optional nature of cyberspace in contrast to the other domains. The four physical do not exist independently from each other and have areas of overlap. Large enough effects in one domain can have effects in another. For example, a change in sea level will have effects in the land domain. Cyberspace, while entirely reliant on the other physical domains, in and of itself, has no direct influence on them.

Despite the increasing influence, control, and connectedness of society and the tools of war through cyberspace, an actor still must choose whether to act within

¹ Douhet, 206.

cyberspace, or at least severely limit their activities within the domain. Because it involves a conscious choice, cyber operations will most likely not become an equal warfighting domain as the physical domains have become. Cyber operations will have to have clear and unambiguous strategic-operational rational to be included in future military planning.

Time and Space Effects of Cyber Operations

A key factor in the decision to conduct cyber operations is defining the strategic objective to achieve an intended outcome. A key precept is that the nature of cyberspace lends itself to the creation of operational time and space. On September 6, 2007, Israeli forces conducted an airstrike with non-stealth aircraft, destroying a secret nuclear facility in Syria. The aircraft accomplished this mission without detection by Syria's advanced air defense radar systems because a corruption-type cyberattack preceded the attack with the effect of showing Syrian air defenders "empty skies" even as the attack was underway.² Cyber operations in effect created the operational space and time to maneuver to achieve the intended strategic effect of destroying the nuclear facility.

In August of 2008, Russia employed a distributed denial of service attack against Georgian government networks prior to moving forces into Georgian controlled South Ossetia. The effect of this cyberattack was the disruption of Georgia's operational command and control, thus creating a time lag in Georgian decision making to enable Russian forces to enter South Ossetia largely unopposed and achieve their desired strategic effect.³

The two examples above demonstrate that cyber operations, when understood as

² Clarke and Knake, 1-6.

³ Libicki, 12.

an integrated part of a strategic-operational intent, can be an effective means of achieving strategic effects. These results are based on an understanding the nature the domain and the principles of operations within the cyberspace.

Targeting Intimacy

Joint Publication 3-60, Targeting, defines a target as an entity or object that performs a function for the adversary considered for possible engagement or other action. Furthermore, Joint Publication 3-12, Cyberspace Operations, states that units conduct cyber operations in support of target objectives, or sequentially or simultaneously support operations in the physical domain to achieve objectives.⁴ Because cyberspace exists within the information environment, it can influence the physical, informational, or cognitive dimensions.⁵

To achieve the desired strategic-operational outcomes, cyber operations require a level of knowledge representing an intimacy not often required for kinetic targeting in the other domains. The dynamic and synthetic nature of systems in cyberspace makes targeting extremely complicated. For example, a control system for one type of structure, such as a power plant, can be vastly different from that of another power plant, even one in the same country. The different types of data processing systems and other architecture amplify the complexity of the overarching system. The intimacy reflects the variety of software and hardware combinations down to the individuals who write the code for these systems. These examples illustrate the level of intimate knowledge necessary to be in a position to target a cyber system.

An example of the level of intimacy necessary for an attack is the Stuxnet attack

⁴ Headquarters, Joint Staff. (2013). Cyberspace Operations (JP 3-12(R)), I-5.

⁵ Headquarters, Joint Staff. (2013). Cyberspace Operations (JP 3-12(R)), I-5.

against the nuclear enrichment facility at Natanz, Iran that resulted in destruction of centrifuges thus delaying the Iranian pursuit of sufficient material to construct a nuclear weapon. This setback may have led Iran to negotiate the Joint Comprehensive Plan of Action that brought the program to a halt. The cyber tool responsible for causing the malfunction that destroyed the centrifuges was later discovered on systems outside the enrichment facility, but there were no recorded incidents of it causing any other malfunctions. This indicates the specific design of the tool to attack the particular supervisory control and data acquisition system that controlled and monitored the equipment in the facility. Furthermore, the specific configuration of the controller and centrifuges in the facility required further tailoring. The target intimacy necessary to accomplish such a surgical attack required development over an extended period of time; requiring levels of technical detail not often required for targeting in other domains. Additionally, the actual source of the attack remains officially unknown.⁶ An added strategic-operational utility of cyber operations is the ability for anonymity or at least the ability to deny responsibility, depending on the strategic outcome desired.

In the same manner, cyberattacks with intended effects in the cognitive dimension require gaining significant and intimate knowledge of the psychological and social makeup of the target. Cognitive targeting, if well executed, will shape the intent and decision making of an adversary. In this way, cyber operations achieve their most significant purpose: to shape decisions and limit options of an adversary, and give all advantages to the attacker who confronts the adversary with the choice of surrender or destruction.

⁶ Though officially unknown, it has been widely suggested that the attack was a combined U.S. and Israeli effort.

In the lead up to the 2003 invasion of Iraq, U.S. cyber operators gained access to Iraq's closed messaging system. A message sent to key military leaders informed them that the U.S. only wanted to remove Saddam Husain and his sons from power. The message informed them that they would not be pursued if army units abandoned their equipment and left their areas of responsibility.⁷ Though this attack resulted in numerous troops leaving their posts just prior to the initiation of the invasion, it is not unreasonable to assume that it also created a level of distrust for the validity of subsequent messages sent in the system and caused doubt in Iraqi command and control efforts.

This example offers an insight into the possible effects from direct information targeting of leaders. In a surgical application, an operation can deliver targeted information or disinformation to a key leader over time, through numerous cyber-based sources to either confirm or refute a specific bias and attain a desired behavior or lead to a specific action that favors the operational outcome.

Advantage of Proximity

A fourth precept of operations in cyberspace is the relationship of proximity to the ability to execute effective attacks. There are two types of proximity with regard to these operations: virtual and physical. A common perception is that cyberattacks are initiated remotely, or virtually, distant from the physical location of the target. This is how the Israelis and Russians initiated their attacks. It is important to understand that though remote access may often be used, it is often necessary to have direct physical access to a system due to its isolation from the rest of cyberspace. In the Stuxnet attack discussed above, a removable thumb drive delivered the tool directly to key equipment

⁷ Clark and Knake, 9-11.

because the system was not connected to outside networks. In this case, not only did the attack rely on intimate knowledge of the system, but it also required physical delivery of the tool to the target.

Key Concepts

To take full advantage of cyberspace it is important for planners to understand how to use the domain for advantage. Strategic advantage often determines the choice to use cyberspace as a warfighting domain. The ability of cyber to create operational time and space, as well as targeting intimacy requirements, and proximity factors must be factored into operational considerations. By understanding these precepts, operational artists can adapt to the changing character of war that has resulted from the creation of the first synthetic domain.

CHAPTER 6: AN OPERATIONAL CONCEPT FOR CYBERPOWER

Cyber has brought with it not only the emergence of a new and useful technology for the conduct of warfare, but it has also for the first time created new operational domain. In the past, new technology has resulted in new thinking and new concepts to take advantage of the existing physical domains of land, maritime, air, and space. The same is required to take advantage of the synthetic domain of cyberspace. This domain provides key opportunities to gain strategic and operational advantages for the operational artist who effectively incorporates cyber power as part of operational design. Daniel Kuehl defines cyber power as the “ability to use cyberspace to create advantages and influence event in the operational environments and across the instruments of national power”.¹

Cyberspace Lessons from Early Maritime and Air Theorists

The determinants first put forth by A.T. Mahan in his *Influence of Sea Power Upon History* offer a pathway to take advantage of cyberspace. Unlike reliance on the accidents or gifts of natural geography in the development of sea power, those wishing to develop cyber power have the opportunity to take advantage of the synthetic nature of the domain and design the physical geography to meet their needs. In doing so they can still apply Mahan’s dictum that physical control provides strategic-operational advantage. For cyberspace, that means ensuring physical control over key nodes and communications architecture linked to cyberspace. This allows can control the quality of access and capabilities, while ensuring that infrastructure is protected.

¹ Daniel T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 24-40 (University of Nebraska Press, 2009), 35.

To take full advantage of the opportunities of cyberspace, those state desiring to become cyber powers must take into account the human aspects necessary for achieving this power. Cyber power, like sea power, is reliant on a population that desires to, and is capable of, operating in the domain. This development will likely be rooted in the desire to gain commercial advantage in cyber space, in ways similar to Mahan's argument for maritime power. Government sponsorship will also be required for the state to be able to take full advantage of the cyberspace domain both commercially and militarily.

Because they are both results of technological advancements, the air and cyberspace domains share many similarities. Giulio Douhet described the theoretical use of air power to change the concept of maneuver in warfare by transcending physical boundaries. Cyberspace also transcends boundaries, existing independently from physical limits. Cyberspace and the air domain also share an offensive oriented nature and the ability to attack military, civilian, and government targets directly.

Similar to Douhet's proposition that air power would lead to victory, the ability to employ cyber power can afford a marked advantage in future conflicts. Like air power, cyber power can be both offensive and defensive – attacking key enemy vulnerabilities while protecting one's own vulnerabilities. Its employment is also most effective in conjunction with other capabilities. The low cost of entry into the cyberspace will result in many state and non-state actors having greater influence against an enemy without operating in any other domain. Whereas there is no equivalent weapon to Douhet's battleplane, the notion of dual-purpose tools shared by governments and the private sector is a key aspect of cyber power. Because cyberspace does not conform to a Westphalian structure of national borders, all those who operate in have the responsibility

to provide security in a way that resembles herd immunity practices that drive mass inoculations.

Operational Concepts

The cyberspace exists both within and separate from the physical domains. As it label suggests, the physical layer exists within the physical domains and is subject to the laws that govern the physical world. However, the logical and data layers are subject to laws created by humans and therefore subject to change and modification. The final layer, the social interaction highlights the importance of the human aspects of cyberspace and reminds the operational artist that in the end the target of warfare in all domains is to influence decision makers.

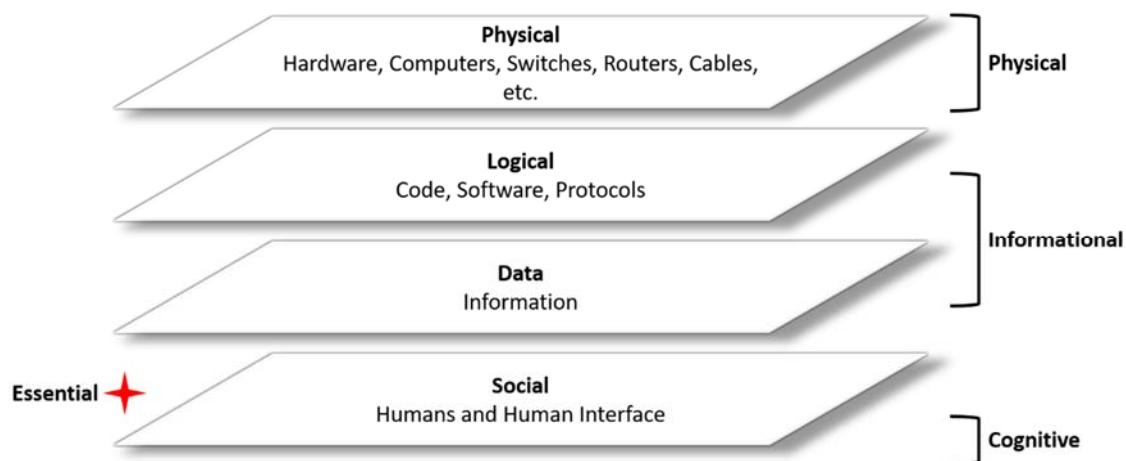


Figure 2 The Four Layers of Cyberspace

All cyberspace systems rely on these four layers to function in the domain. A reconnaissance effort is necessary to reveal these layers and map their activities – in the same way any conventional reconnaissance unit would locate and report on activities of an enemy force. The layers are revealed and understood in terms of how they support specific joint functions (state based adversaries) or critical enablers (non-state actors). It is now possible to apply degrees of cyberattack to the enemy cyber system to create

specific effects integrated into operational phases, or can be employed as a single strike option to prepare the battlespace, or serve as an operational reserve in support of an offensive or defensive maneuver. Categorizing and describing the degree of attack and articulating the desired operational effects allows cyber power to be employed in sequence in time and space with other components in other domains to achieve the decisive effect.

When planning cyberspace operations it is necessary first to understand the layer or layers in which the desired effects are to be realized. For conventional targetiers, the physical layer will be the most familiar. Since this layer exists in the same space as the physical domains, the same techniques to effect it are available to operational artists. In addition, cyber delivered means can affect the domain.

Both the logic and data layers of the cyber domain exist in the information environment and therefore are targetable only through cyber means. To effect these layers, the objective is to alter the code or corrupt the data that resides here. The logical and data layers of key technology based infrastructure and industrial capabilities of a state, such as electrical grids and the financial sector, will often be the target in conjunction with the morale of the population in an effort to disrupt the industrial capabilities and trinitarian relationship between the government, military, and population. Often this will be accomplished by directly targeting the physical layer where human access takes place.

Finally, on the social layer the target is the enemy cyber operator. Those who conduct on net operations, those who develop tools for offensive operations, and those charged with maintaining the defensive aspects of a system are all possible targets.

Cognitively and kinetically targeting these individuals will have the effect of rendering a cyber force ineffective.

The operational tasks to create the effects described above are to interdict, disrupt, corrupt, or destroy the target. By using these commonly understood terms, operational artists can employ cyber effects through sequential or singular operations by phase according to operational design. Through the combination of effects in, operational artists can achieve strategic-operational goals.

Conclusion

The study of the above theorists combined with early strategic and operational uses of cyberspace highlights a number of concepts operational artists can use when coordinating operations across all domains. Though the state that chooses not to take advantage of cyberspace does so at its own peril, the synthetic nature of cyberspace does ultimately mean that operations within it are optional. The nature of modern military and societal technology makes this option less and less likely. It is still important to identify the opportunities, choosing to operate in cyberspace present, while understanding that these actions may not be decisive but support other decisive actions.

Along this line of reason, cyber operations afford the operational artist the ability to create advantages in time and space for the traditional operations conducted in the physical domains. Cyber effects can result in the technological equivalent of smoke screens against an adversary who is reliant on technology for decision-making. It can also be a means to sabotage key enemy capabilities to provide room for negotiated outcomes and thus prevent possible physical violence. In order to achieve these effects, cyber operations will require a much more detailed understanding of the target, either systems

or humans, than was typically required for more traditional targeting efforts. Finally, the operational artist needs to understand the importance of both physical and network proximity in gaining effects. Ultimately, cyber operators need to be able to gain access to systems to be able to affect them.

When technological developments result in changes in the character of war, a review of historical examples of others who have dealt with similar changes should also follow. This historical examination in the context of cyberspace has identified a number of key concepts for planners to take into account when seeking advantage in the domain. To paraphrase the quote that opened this paper, *cyberspace has opened up a new field of action and created a new battlefield*.² Operational artists need to remember that where humans encounter each other in this domain, conflict will result. The outcome will be in the favor of those who can apply the lessons of history and apply new concepts learned from them.

Based on review of the methodology outlined in the analytical model that describes the nature of the domain, the precepts that lead to the conceptual theory and the operational concept for cyber power followed by the outline and discussion of the operational concept

² Douhet, 3.

BIBLIOGRAPHY

- Alexander, Keith B. "Warfighting in Cyberspace." *Military Technology* vol. 35, no. 3 (March 2011)03: 41-45.
- Bailey, Richard J., Jr. "Four Dimensions to the Digital Debate, How Should We Think Strategically about Cyberspace and Cyberpower?" in *Strategy: Context and Adaptation from Archidamus to Airpower*, 186-207. Annapolis, MD: Naval Institute Press, 2016.
- Barcomb, Kris E. "From Sea Power to Cyber Power." *Joint Force Quarterly*, no. 69 (2nd Quarter 2013): 78-83.
- Blowers, Misty ed. *Evolutions of Cyber Technologies and Operations to 2035*. New York: Springer Cham Heidelberg, 2015.
- Brodie, Bernard. *The Heritage of Douhet*. Santa Monica, CA: Rand, 1952.
- Clarke, Richard A. and Knake, Robert K. *Cyber War: The Next Threat to National Security and What To Do About It*. New York: Harper Collins, 2010.
- Dallek, Matthew. "To Understand the Future of Cyber Power, Look to the Past of Air Power." *Huffington Post*, March 30, 2017. https://www.huffingtonpost.com/entry/cyber-war-technology_us_58dbfab2e4b01ca7b4294347.
- Douhet, Giulio. *Command of the Air*. North Stratford, NH: Ayer Company, 1942.
- Fahrenkrug, David T. "Cyberspace Defined." Australian Air University. http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm (Accessed October 28, 2017).
- Forsling, Carl. "Should Cyber Warfare Have Its Own Branch?" *taskandpurpose.com*, <https://taskandpurpose.com/cyber-warfare-branch/> (Accessed October 28, 2017).
- Garamone, Jim. "U.S. Commanders Must Embrace Cyber, Special Ops Chief Says." DoD News, Defense News Agency, December 13, 2017. <https://www.defense.gov/News/Article/Article/1396033/us-commanders-must-embrace-cyber-special-ops-chief-says/> (accessed on December 16, 2017).
- Garamone, Jim and Ferdinando, Lisa. "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command" DoD News, Defense News Agency, August 18, 2017. <https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/> (accessed on February 15, 2018).
- Gartzke, Erik. "The Myth of Cyberwar, Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (Fall 2013): 41-73.

- Gibson, William. *Burning Chrome*. London: Gollancz, 1986.
- Greathouse, Craig B. "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter." in *Cyberspace and International Relations Theory, Prospects and Challenges*, 21-40. Bonn, Germany: University of Bonn, 2014.
- Hansen, Andrew P. "Nothing New Under the Sun: Benefiting from the Great Lessons of History to Develop Coherent Cyberspace Deterrence Strategy." Master's Thesis, National Defense University, Joint Forces Staff College, Joint Forces Staff College, Joint Advanced Warfighting School, 2012.
- Headquarters, Joint Staff. (2013). *Cyberspace Operations (JP 3-12(R))*.
- Headquarters, Joint Staff, (2017), *DOD Dictionary of Military and Associated Terms*.
- Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 24-40. University of Nebraska Press, 2009.
- Kern, Sean C. G. "Expanding Combat Power through Military Cyberpower Theory." Master's Thesis, National Defense University, Joint Forces Staff College, Joint Advanced Warfighting School, 2015.
- Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. New York: Penguin Press, 2017.
- Lamothe, Dan. "How the Pentagon's Cyber Offensive Against ISIS could Shape the Future for U.S. Forces." *The Washington Post*, December 16, 2017.
- Leonard, Robert R. *The Principles of War for the Information Age*. Novato, CA: Presidio Press, 1998.
- Libicki, Martin C. *Cyberspace in Peace and War*. Annapolis, MD: Naval Institute Press, 2016.
- Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York: Frank Cass, 2004.
- Lorber, Azriel. *Misguided Weapons: Technological Failure and Surprise on the Battlefield*. Washington, D.C.: Brassey's, Inc., 2002.
- Lucas, Edward, Nimmo, Ben. "Information Warfare: What Is It and How to Win It? CEPA Inforwar Paper No. 1" Washington, D.C.: Center for European Policy Analysis, November 2015.
- Mahan, A. T. *The Influence of Sea Power upon History, 1660-1783*. Mineola, NY: Dover, 1987.

Morrow, Nicholas, "Giulio Douhet, The Command of the Air (1921/1927)." *Classics of Strategy*, <http://www.classicsofstrategy.com/2015/09/the-command-of-the-air-by-giulio-douhet-19211927.html> (accessed on December 16, 2017).

Mulford, Laurie A. *Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. Cyber Command*. Master's Thesis, National Defense University, Joint Forces Staff College, Joint Advanced Warfighting School, 2013.

Olsen, John A. *A History of Air Warfare*. Washington, D.C.: Potomac Books, 2010.

Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.

Senatore, Holly. "Giulio Douhet's Command of the Air: Designing the Principles for Cyberwar in the 21st Century." *Military History Online*. <http://www.militaryhistoryonline.com/general/articles/cyberwar21stcentury.aspx> (accesses December 16, 2017).

Smith, Rupert. *The Utility of Force*. New York: Alfred A. Knopf, 2007.

Tadjdeh, Yasmin. "SOCOM Commander: U.S. Must Develop More Offensive Cyber Weapons." *National Defense*, December 14, 2017.

United States Department of Defense. "Department of Defense Strategy for Operating in Cyberspace." (2011).

United States Department of Defense. "Department of Defense Dictionary of Military and Associated Terms." Washington, D.C.: Dept. of Defense, 2017.

Vergun, David. "Commanders Need Latitude to Employ Offensive Cyber, Says GEN Thomas." *Army News Service*, December 12, 2017.

Warner, Edward. "Chapter 20: Douhet, Mitchell, Seversky: Theories of Air Warfare." In *Makers of Modern Strategy: Military Thought from Machiavelli*. Edited by Edward Mead Earle, 485-503. Princeton: Princeton University Press, 1948.

Waterman, Shaun. "Elevation of Cyber Command Will Make It More Like Its Elite Brethren." *Cyberscoop*, August 29, 2017, under "Government," <https://www.cyberscoop.com/cyber-command-socom-training/> (accessed on December 19, 2017).

Welch, Larry D. "Cyberspace - the Fifth Operational Domain." *Institute for Defense Analyses Research Notes*, (Summer 2011) <https://www.ida.org/idamedia/Corporate/Files/Publications/ResearchNotes/RN2011/2011-Cyberspace---The-Fifth-Operational-Domain.pdf> (accessed October 28, 2017).

Wentz, Larry K., Stuart H. Starr, and Franklin D. Kramer. *Cyberpower and National*

- Security*. Washington, D C: Potomac Books, 2009.
- Williams, Brett T. "Ten Propositions Regarding Cyberspace Operations." *Joint Force Quarterly*, no. 61 (2nd Quarter 2011): 11-17.
- Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly*, no. 73 (2nd Quarter 2014): 12-19.
- Witte, John C. "The Panacea and the Square Peg: Strategic Fallacies of the Air, Undersea, and Cyber Domains." Master's Thesis, National Defense University, Joint Forces Staff College, Joint Advanced Warfighting School, 2015.
- Yong-Soo Eun, and Judith Sita Aßmann. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." *International Studies Perspectives* 17, no. 3 (2016): 343-360.
- Zittrain, Jonathan. *The Future of the Internet - and How to Stop It*. New Haven, CT: Yale University Press, 2008.

VITA

Lieutenant Colonel Sean C. Heidgerken is currently assigned to the Joint Advanced Warfighting School (JAWS) at the Joint Forces Staff College in Norfolk, VA. Colonel Heidgerken received his commission from Army Officer Candidate School in 1998 as a Field Artillery Officer. He now serves as an Information Operations Officer with tactical and operational experience in both conventional and Special Operations units. Colonel Heidgerken has served in OPERATIONAL IRAQI FREEDOM (OIF) and OPERATION INHERENT RESOLVE (OIR). His previous assignment was as the Combined Joint Task Force Operation Inherent Resolve Deputy Director of Information Operations where he was responsible for the planning and integration of Information Operations, Cyber Operations and other sensitive operations. He will be assigned to the U.S. Central Command following graduation. Colonel Heidgerken is a graduate of the U.S. Army's Command and General Staff College and a former fellow with the Kansas City Chiefs Media and Production Department.