

Air Force Institute of Technology

AFIT Scholar

---

Theses and Dissertations

Student Graduate Works

---

12-18-2008

## Cyber Power in the 21st Century

Joseph M. Elbaum

Follow this and additional works at: <https://scholar.afit.edu/etd>



Part of the [Databases and Information Systems Commons](#), and the [Information Security Commons](#)

---

### Recommended Citation

Elbaum, Joseph M., "Cyber Power in the 21st Century" (2008). *Theses and Dissertations*. 2530.  
<https://scholar.afit.edu/etd/2530>

This Thesis is brought to you for free and open access by the Student Graduate Works at AFIT Scholar. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of AFIT Scholar. For more information, please contact [richard.mansfield@afit.edu](mailto:richard.mansfield@afit.edu).



**CYBER POWER IN THE 21<sup>ST</sup> CENTURY**

THESIS

Joseph M. Elbaum, AD-21, USAF

AFIT/GCO/ENG/09-01

**DEPARTMENT OF THE AIR FORCE  
AIR UNIVERSITY**

***AIR FORCE INSTITUTE OF TECHNOLOGY***

---

**Wright-Patterson Air Force Base, Ohio**

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GCO/ENG/09-01

**CYBER POWER IN THE 21<sup>ST</sup> CENTURY**

THESIS

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science (Cyber Operations)

Joseph M. Elbaum, AAS, BS

AD-21, USAF

December 2008


APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

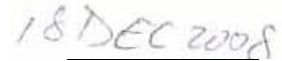
**CYBER POWER IN THE 21<sup>ST</sup> CENTURY**

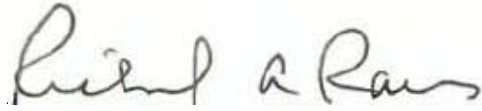
Joseph M. Elbaum, AAS, BS

AD-21, USAF

Approved:

  
Robert F. Mills, PhD (Chairman)

  
Date

  
Richard A. Raines, PhD (Member)

  
Date

## Abstract

Historically, the United States Congress has acknowledged that a separate branch of military service is required to exert supremacy over each of the recognized Domains of Operation. Throughout the evolution of modern warfare, leading minds in military theory have come to the conclusion that due to fundamental differences inherent in the theory and tactics that must be employed in order to successfully wage war within a domain's associated environment, a specialized force was needed - until now. With the recent inclusion of Cyberspace as an operational domain by the Department of Defense, the case should be made that it, too, is far too specialized an area to be rolled up into any or all of the current branches of service.

This research investigated the concept of cyber power in the 21<sup>st</sup> century, what it means to wield it, and how this capability may be used to wage war. It argues that cyberspace as a domain should be treated no differently than the traditional warfighting domains: that it, too, is an arena where defense may best be secured by attacking the enemy, where battles occur for control of territory, where denial affects combat in other domains, and where political motives dictate the course of hostilities. Because the strategic challenges and concepts are the same and yet the environment so specialized, the research concludes that the only way to properly secure the domain and to prosecute war effectively is to create a U.S. Cyber Force.

*To my wife, without whose love, patience, and understanding this paper  
would not have been possible*

## Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Robert Mills, for his guidance and support during this long process. It was his infectious enthusiasm for the subject which caused me to choose it as the topic of my thesis. I would also like to thank all of the other numerous AFIT faculty and staff who answered my questions, pointed me in the right directions, and generally put up with me during the evolution of this research. And finally, I want to thank my parents for always emphasizing the importance of a good education.

Joseph M. Elbaum



## Table of Contents

	Page
Abstract.....	iv
Acknowledgements.....	vi
Table of Contents.....	vii
List of Figures.....	ix
List of Tables.....	xi
I. Introduction.....	1
Motivation.....	1
Problem.....	2
Objectives.....	3
Approach.....	3
Results.....	4
Document Overview.....	4
II. A Service for Every Domain.....	6
What are Domains?.....	6
Why a Separate Army and Navy?.....	9
Along Came Air.....	13
...and Space.....	21
Cyberspace Emerges.....	26
III. The Nature of Power and Dominion.....	37
What is (Military) Power?.....	37
Theories of Military Power.....	45

Power on Land .....	45
Power at Sea.....	54
Power in the Air and Space.....	66
IV. Cyber Power in the 21 <sup>st</sup> Century.....	75
Clarifying the Environment .....	75
Power in Cyberspace.....	77
Elements of Cyber Power .....	79
Tenets of Cyber Power.....	81
Cyber Operations .....	84
Propositions Regarding Cyber Warfare .....	86
V. Conclusions and Recommendations .....	95
Research Overview .....	95
Conclusions and Significance of Research.....	95
Recommendations for Future Research .....	95
Summary .....	96
Bibliography .....	97
Vita.....	104

## List of Figures

Figure	Page
1 – The Five Warfighting Domains .....	6
2 – The Machine Environment .....	31
3 – Fundamentals of Full Spectrum Operations .....	50
4 – The Well-Worn Paths of Cyberspace: Undersea Cables .....	56
5 – The Well-Worn Paths of Cyberspace: Internet Backbones .....	57
6 – The Well-Worn Paths of Cyberspace: Critical Communications Satellite .....	58
7 – Fundamentals of Full Spectrum Cyber Operations.....	78

## List of Tables

Table	Page
1 – Actor Center of Gravity Dependence .....	40
2 – Asymmetric Effects of Cyber Warfare .....	41

# CYBER POWER IN THE 21<sup>st</sup> CENTURY

## I. Introduction

### Motivation

There exist today many papers, books, and articles that explore and assert what one must *do* to secure and operate in the wild frontier-land of cyberspace. As the advent of cyberspace and then cyber war manifested itself, scholars began crafting numerous documents which tried to come to terms with the subject. These writings do an admirable job at describing the threats and how to counter them, such as Edward Waltz' book Information Warfare: Principles and Operations, Gregory Rattray's Strategic Warfare in Cyberspace, or Martin C. Libicki's Defending Cyberspace and Other Metaphors. Some writings even go so far as to detail policy the writer thinks should be adopted; but the common theme for all of these documents is to place the onus for enacting these suggested tactics and policies on an unnamed and undefined shadowy government entity. Who should be doing this work? Whose responsibility is it to protect our nation's cyberspace? The Air Force announced in 2005 that it would "fly and fight in air, space and cyberspace" [86] and began organizing, training and equipping a cyber force. The Air Force's focus has changed slightly: rather than creating a new major command (MAJCOM) dedicated to cyberspace, Air Force leaders have decided to put cyberspace operations under Air Force Space Command. [2] However, the Air Force mission retains a strong (perhaps stronger) emphasis on cyberspace: "The mission of the Air Force is to fly, fight, and win in air, space and cyberspace." [22]

The Army and Navy have taken similar steps. In the case of the former, the Army's Land Information Warfare Activity was re-designated the 1<sup>st</sup> Information

Operations Command in 2003 to: “deploy information operations support teams in order to provide IO planning support and vulnerability assessments in support of military forces and provide an IO reach-back capability to operational and tactical IO staffs as directed;” [68] and in the case of the latter, Navy brass began laying the groundwork to build a Naval Cyber Force Command around their existing Naval Network Warfare Command whose mission is to “deliver integrated cyber mission capabilities in Information Operations, Intelligence, Network Operations, and Space that enable warfighters across the full range of military operations” sometime in 2007. [7, 20] Clearly, each service recognizes the need to master this new domain, but the creation of so many entities threatens to pull the nation’s capability in too many directions at once.

This document is different. It will not describe tactics or policies for securing or operating in cyberspace. Rather, this is a document designed to make one think and provoke discussion. It will draw lessons from both American history and the great military minds of various other countries and apply them to what is happening with cyberspace today.

### **Problem**

This research studied the reasons behind the establishment of a separate Army, Navy, and Air Force; the ways in which each service derives power from strategy in its respective operational domain; and how a notional Cyber Force might derive power in cyberspace through strategies of its own. The answers to these questions are of the utmost importance in determining whether the creation of a separate Cyber Force is necessary to ensure ongoing American superiority in the domain.

## **Objectives**

The objectives of this research include establishing that cyberspace is, like the other operational domains, too specialized a field to leave its mastery up to any or all of the current branches of military service; to provide insights into how the traditional and contemporary strategies of warfare used in other domains may be applied in cyberspace; and to propose a comprehensive set of ideas, tempered by precedent and research, which may be used in the formulation of a new Cyber Force's strategy and doctrine. The sum total of these objectives will show that a separate Cyber Force is required for American dominance of cyberspace in the 21<sup>st</sup> Century and beyond.

## **Approach**

To achieve the above listed objectives, one need only look to precedent and example; both of the past and the present. The answer to who should take charge of cyberspace resides (as it usually does) within the lessons of previous successes and failures. There is strong precedent for a separate service to oversee each of the domains of operation. The reasons are many and diverse, but ultimately come down to strategy. The last service to come into existence in order to master a domain, the Air Force, was born of strategy; first high altitude precision daylight bombing and then global nuclear deterrence. While other services—such as the Navy—may also utilize aircraft to accomplish their missions, marine aviation is more a source of fires (akin to artillery) and is largely fleet-centric. The Air Force is considered the lead entity for the Air, and only it looks at air superiority from a domain control/denial standpoint. Current writings on cyber power, however, do little to address strategy even though it is now recognized as the newest warfighting domain. These writings are too far “down in the weeds,” and

speak specifically of tactics and policy that current services should pursue but lack greatly in describing where, why, when, and how such tactics and policy should be used or applied.

## **Results**

The research revealed that the reasons for the creation of a Cyber Force are just as valid, if not more so than the reasons the three current branches of service to exist today. Additionally, the research revealed that cyber power shares many common ideas and nuances of strategy with operations in the other domains which may be applied in order to better understand the derivation of power and application of warfare in the cyber domain. Finally, the research also revealed some sound principles and underlying truths of operations in cyberspace which may be used in order to shape future strategy. The culmination of these findings strongly suggests the creation of a United States Cyber Force.

## **Document Overview**

The remainder of this document will describe the research in more detail and is structured as follows. Chapter II will start with describing what a domain is and why differing environments call for different strategies. It will make the case that a separate service is needed to prosecute each of these different strategies based upon the different laws of nature inherent to each environment. Chapter III will go on to describe what these strategies for gaining and applying power are within each of the previous four domains and discuss their respective services' methods for successful operations. Additionally, it will synthesize and apply those lessons that can be taken from the other services' strategies for dominion to cyberspace and discard the ones that cannot. Chapter



IV will display an aspect of cyber power and cyber strategy that emerges from the preceding discussions, which in turn should make a strong argument and basis for the creation of a separate yet equal branch of the Department of Defense. Finally, Chapter V will conclude with a summary and recommendations for future research that may be of use to one establishing a separate U.S. Cyber Force.

## II. A Service for Every Domain

### What are Domains?

“Domain” is a word which is often used in the Defense community when discussing the individual and complex spheres in which combat operations may occur. Interestingly enough, despite such common usage there are no formal Department of Defense definitions put forward for the word. However, it is generally understood that (in a military sense) a domain is a place where activities are performed to achieve some level of influence or control. This assumes that there are other actors (hostile, neutral, or benign) who also operate in the domain and wield some influence—if only to protect their own ability to operate.

Taken in the context with which it is used in innumerable DoD documents, we may infer that out of the 10 entries listed in the dictionary under “domain,” there are two which, when melded together, properly describe the word as it relates to warfighting and the military profession. These two definitions are “a region distinctively marked by some physical feature,” and “a territory over which dominion is exercised.” [21]

The commonly accepted and understood military “warfighting domains” are land, sea, air and space. [51] However, doctrine only defines two of them, and both definitions are problematic. Land, Sea, and Air do not receive DoD definitions, and Space is defined as: “A medium like the land, sea, and air within which military activities shall be conducted to achieve US national security

### The Five Warfighting Domains

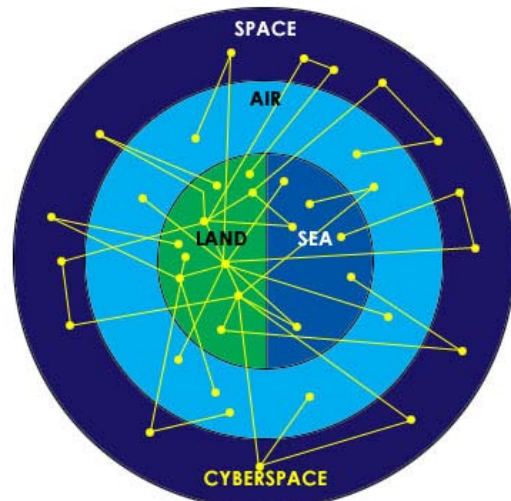


Figure 1 - Cyberspace exists across and affects objects in the other four domains

objectives.” [74]. These first four domains are within the human experience: we can sense them and interact within those domains daily. Therefore they are somewhat self-explanatory.

Cyberspace is different. It involves physical equipment and technology, but much of it has a virtual aspect. This makes it difficult to explain in terms that are on par with the other warfighting domains. For this reason, there have been many attempts to define what exactly cyberspace is, and these definitions change over time. Within the Department of Defense alone, establishing a clear understanding of *what's in* and *what's not* has proven difficult. This is not a new problem: many of the fundamental ideas about cyberspace trace back to the early 1990s when information warfare (IW) attracted a lot of attention as a new way of fighting wars, but these concepts were abstract and difficult to integrate with traditional physical/kinetic operations. More recently, the National Military Strategy for Cyberspace Operations (NMS-CO), published in 2006, defined cyberspace as “a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure”. [80] This definition, while rather broad in scope, is at least grounded in physics and allows for more direct comparison with the other physical domains of warfare.

An even more recent official Department of Defense definition was released in May 2008: “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” [26] Although this definition places emphasis on the Internet, it includes wireless networks, tactical data links, and any other network through which information is shared.

This most recent definition of cyberspace seems to emphasize the technology aspects of the domain. This is true of all of the domains, since military operations are increasingly dependent on technology to exploit and control the domain. The maritime domain could not be effectively controlled until man could build suitable vessels; likewise prior to powered air- and spacecraft, controlling the air and space domains would not have been possible. The land domain is also largely dependent on technology (artillery and armor), although a society that does not have advanced technology can still wield some influence, even if it is with rocks and spears.

Although cyberspace may have a physical infrastructure, much of the cyber domain exists within virtual spaces that we cannot perceive with our five senses. The only way that humans may interact with and influence these areas of the fifth domain is through the use of tools which harness the power of the electromagnetic spectrum in order to send commands across networks to be interpreted by man-made machines. This virtual space is not a realm into which humans may enter. As a result, these repeated attempts to define the domain have floundered.

Another reason Cyberspace is so ambiguous in the human mind is that of the five domains, cyberspace is in effect a man-made domain. Clearly, the electromagnetic spectrum is not man-made, but the information systems that make up the cyberspace environment are man-made. Without routers and switches and radio transmitters, there is no need to try and discuss cyberspace as a warfighting domain. Humans have created the domain, primarily to support and enable operations in the other domains. Because of this, warfighters will need to protect their own ability to use the cyberspace domain, while hindering an adversary's ability to do so. This contest for control and influence is what it means to have cyberspace as a warfighting domain.

Of the five domains, Land seems to be the least technology-dependent. Cavemen could have squabbles over who had the best caves, relying on their fists, feet, and teeth they were born with.

After the domain of Land, which has always existed, came the domain of Sea. While the environment the domain would eventually encompass had always existed, the technology to exploit it did not. It took the invention of the ship before dominion could begin to be exercised over the high seas. It is not known when the first ships were invented, but, there are depictions of pole barges in Egypt that are at least 6,000 years old, and evidence exists that the Greeks and Phoenicians invented galleys sometime between the years 1200 to 900 BC. [55] Regardless of the exact date, the warfighting domain was created as soon as technology for controlling the maritime environment was available.

### **Why a Separate Army and Navy?**

To summarize, a domain is “a region distinctively marked by some physical feature” [21] over which humans attempt to exert control or dominance. Given this understanding of a warfighting domain, let us explore why separate military branches (services) have evolved to properly exploit each domain. One reason is that the nature of the environment itself is unique for each case. For example, the land and sea environments are characterized by similar features such as climate and geography, but they differ greatly in how we move about (operate) within the environment. Physics concepts such as gravity, force, acceleration, kinetic and potential energy govern the motion of bodies in each domain. There may be some similarities across the domains, but each has its own tenets, principles, technologies, and doctrine for operating in that environment. Merely possessing the technology (tools) is not enough to contest a warfighting domain. Potential adversaries and competitors may also wish to exercise dominion over an

environment to protect or promote their interests. Preserving the ability to operate (and prevail) in a domain then involves developing technologies that remain ahead of or at least on par with those of any potential adversary—in essence an arms race.

Effective employment of technologies requires an intimate knowledge of the environment in order to create a sensible strategy that makes use of good tactics and technology that are specially tailored to the environment. Assuming equivalent technologies exist, superiority in a domain may very well depend on which side better understands how to fight in that domain. It is possible to appoint leaders and recruit people to draft strategy and execute operations in environments they do not fully understand, but this practice would likely lead to defeat against a more experienced adversary. In fact, there have been numerous cases where superior technology was either nullified or defeated through superior doctrine and tactics.

In 1775, a coalition of thirteen former British colonies found themselves in need of an armed, land-based force to prosecute their rebellion against the tyranny of English rule. And so it was that on June 14th, the newly formed Second Continental Congress adopted “the American Continental Army.” Provisions were made for the recruitment of ten companies of riflemen, along with a requirement to draft the necessary enlistment forms and the appointment of a committee to write the rules and regulations for the government of the new army. From that point, the army rapidly expanded in size as the individual colonies’ militiamen were brought under the Continental Army’s umbrella. Troop numbers quickly soared to around 27,000 men towards the end of July of that year, most of which were pressed into the defense of Boston under the Army’s first Commander-in-Chief, General George Washington; the remainder were stationed in New York. [84] General Washington was avidly interested in the military arts from a young age, and had been commissioned a Lieutenant Colonel in 1754 to fight in the beginning

skirmishes of the French and Indian War. The next year, he was assigned to serve as an aide to British General Edward Braddock, which he did until 1759. [57]

Soon after the establishment of the Army, Congress realized that fighting the British on land was all well and good, but there was a need to harry and disrupt their resupply of troops and equipment from across the Atlantic as well. Maritime operations were already being undertaken by the Army; General Washington had taken command of three armed schooners under Continental authority to intercept British supply ships near Massachusetts. However, Congress decided to add yet more ships to this force and establish a separate Continental Navy on the 13th of October, 1775 by authorizing the procurement, outfitting, manning, and dispatch of two additional armed vessels and sending them in search of ships supplying the British Army in America. The Continental Navy eventually consisted of some 50 ships over the course of the war, with approximately 20 warships active at its maximum strength. [18] The legislation drafted by Congress also established a Naval Committee to write the necessary rules and regulations, just as it had with the Army four months earlier, and appointed Commodore Esek Hopkins as the first Commander-in-Chief of the Navy. Commodore Hopkins had been a seafaring man from a young age, captaining merchant vessels and going on to be a successful privateer during the French and Indian War before being appointed to this high office. [17] He seemed an excellent choice for the command.

It is apparent that Washington and Hopkins were chosen to lead their respective services because of the very different training, study, and experiences they had received in their chosen domains. Congress realized that because the nature of Land and Sea were so different, they needed to appoint leaders who were well versed in their environments. Land commanders and troops needed to know about such things as forced marches, supply lines, terrain, elevation,

fighting formations, and volley fire. Naval commanders and sailors needed to understand navigation by sextant, water currents, broadsides, weather, tides, sail trim, tacking, ropes and knot tying, etc. It is doubtful that a naval campaign against the British Navy organized by General Washington would have had the success that the campaign organized by Commodore Hopkins had; nor could we conclude that Hopkins would have been as successful in the ground campaign as Washington.

There is much evidence that strategy and tactics alone won the colonies their independence, and that these stratagems would not have been as effective had they been created by people who did not fully understand their respective domains. The English had more men, more money, better equipment, more combat experience, and the best Navy in the world with 100 Ships of the Line, while the colonists had many forces which were described by one of their own Generals, Philip Schuyler of New York, as “weak in numbers, dispirited, naked, destitute of provisions, without camp equipage, with little ammunition, and not a single piece of cannon.”

[5] Both the Continental Army and Navy were new creations, without tradition or even military experience. [5] However, what the English didn't have was superior strategy and tactics.

General Washington's fighting style is characterized by a letter he wrote to Congress stating:

“we should on all Occasions avoid a General Action, or put anything to the Risque, unless compelled by a necessity, into which we ought never to be drawn.” [57] An example is his

famous nighttime crossing of the Delaware River to surprise and engage the English at the Battle

of Trenton. [57] Meanwhile, the British strategy focused more upon taking and holding coastal

cities through the use of their superior sea power rather than engaging the bulk of the enemy

forces which were mainly garrisoned in the interior and the rural areas of America. [4]



Already, at the very beginnings of our young nation, Congress recognized the fact that a separate force with a separate set of skills, separate chain of command, and a separate way of thinking was required for each domain of operations it was necessary to wage war in, even if they did not yet coin or speak in these terms. Because of the fundamentally different attributes and laws of nature inherent in each of the environments that encompass every domain and the tactics necessary to properly exploit them, this view would prove to be borne out when next it became feasible to wage war in a new domain.

### **Along Came Air... and Space.**

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

*-Gen. Giulio Douhet*

The first military application of airborne technology occurred during the French Revolutionary War, when France utilized a tethered hydrogen balloon to observe the troop movements of the Austrian army at the Battle of Fleurus in 1794. [72] Although lighter-than-air aircraft technology was invented in France, it quickly spread to other countries and was eventually adopted by American military forces in 1861 for use during the Civil War. The technology was employed in much the same way that France had; a stationary, tethered balloon used for reconnaissance and observation of battlefield troop movements. [71] Although these tools were helpful reconnaissance assets, one could not really argue that they allowed for the dominance or control of the air environment.

On December 17, 1903, Wilbur and Orville Wright made history by successfully accomplishing the world's first powered, sustained, and heavier-than-air flight at Kitty Hawk, North Carolina. [66] Now that the technology had been invented that would make possible the dominion of the air, advancements into the warfighting capabilities of this new invention would

progress swiftly. In the following few years, advances occurred in airfoil design, lightweight propulsion systems, aerodynamics, control systems, and weaponry. It should be noted that this rapid progress in airplane technology was mainly the result of a European arms race in the air domain during WWI (American wartime aviation having been deemed a novelty and unnecessary to combat operations by the War Department). [40] During this time, much of each opposing countries' aircraft technology was nearly identical—or at best only marginally superior in one technical area or another. As a result, the two early air power theorists—Italian Giulio Douhet and American Billy Mitchell—believed that defeating an enemy whose technology was at least equal to one's own required superior strategy, tactics, and doctrine. To this end, they continually formulated and expounded their views on the nature of air power, all the time arguing that a separate military branch would be required to fully exploit this new domain.

Their stories are remarkably parallel. Both men leapt at the chance to be a part of the emerging world of aviation in the early 1900's and both argued vehemently with their respective leadership on the role of airpower in warfare. Likewise, both men were subsequently court-martialed for their vigorous criticism of military orthodoxy (in Douhet's case, he was also imprisoned for a year) and then reinstated and promoted to General when their views eventually proved to be correct. [23, 45] General Douhet wrote in his 1921 book "The Command of the Air,"

*Though an army is primarily a land force, it possesses a navigable means of warfare which it can use to help integrate its land operations; and that fact does not preclude the navy's accomplishing, solely with its own naval means, war missions from which the army is completely excluded. Similarly, while a navy is primarily a sea force, it possesses land means of warfare which it may use to assist and integrate its naval operations; and that fact does not preclude the army's carrying out war missions solely with its own land means, entirely independent of any naval means. In like manner, both the army and navy may well possess aerial means to aid and integrate their respective military and naval operations; but that does not preclude the possibility, the*

*practicability, even the necessity, of having an air force capable of accomplishing war missions solely with its own means, to the complete exclusion of both the army and navy.*

*In such case, an air force should logically be accorded equal importance with the army and navy and bear the same relation to them as they now bear to each other. Obviously, both the army and the navy, each in its own field, must operate toward the same objective—i.e., to win the war. They must act accordingly, but independently of each other. To make one dependant on the other would restrict the freedom of action of the one or the other, and thus diminish their total effectiveness. Similarly, an air force should at all times co-operate with the army and the navy; but it must be independent of them both. [23]*

It is at this juncture that I must take a moment to speak about one of General Douhet's hypotheses in the above excerpt: Possessing the means to operate in an environment other than the one to which your service has been assigned in order to accomplish some facet of your mission does not render another service obsolete. The ability to use and exploit an environment in order to achieve goals in some other domain and the ability to wage war and create effects in the new domain are two very different things. Until the air environment was understood well enough to become a warfighting domain, the Army used it to support its other many functions. For example, artillery shells fly through the air, and powered aircraft were also used to observe the battleground and provide situational awareness for ground commanders. But neither of these involves creating effects in the air environment in order to control it or deny an adversary's use of the air environment.

So what, then, constitutes the materiel belonging to a certain domain? Do artillery shells necessarily "belong" to the air domain because they travel through the air? Of course not. They are simply tools, and a tool does not belong to a domain. The things that "belong" to a domain are the doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMLPF). The doctrine includes strategy and tactics regarding the proper employment of warfighting capabilities, usually based on experimentation and lessons learned. Conflicts over

who should “own” a domain usually arise because of the funding and other resourcing constraints when allocating roles and missions.

Continuing the remarkable parallelisms between the two theorists, Mitchell also wrote a book on Air Power published in 1921, titled “Our Air Force.” In it, he wrote:

*No navies can operate on the seas, nor armies on the land, until the air forces have first attained a decision against the opposing air forces, so as to allow those on the water to operate against their enemy. Therefore, as a prelude to any engagement of military or naval forces, a contest must take place for control of the air. The first battles of any future war will be air battles. The nation winning them is practically certain to win the whole war, because the victorious air service will be able to operate and increase without hindrance. Under these conditions, it is essential that they can be mobilized and put into fighting condition immediately that war appears imminent, to take the air and protect the country in the way that it deserves. [45]*

Both men knew that a separate and equal air force whose sole purpose was to focus on perfecting warfare in and from the air was required to adequately protect their respective nations from enemy air forces and take the battle to the enemy from over the front lines. As Billy Mitchell was later quoted, “Just as the navy always thinks first of battleships and makes aviation secondary to that, the army thinks only of the infantry and makes aviation a secondary matter.” [46]

That is not to say that Douhet and Mitchell agreed upon every aspect of war in the Air domain. Douhet’s vision of air power was mainly strategic and offensive in nature, and called for massive bombardment of large population centers in order to demoralize the civilian populace, [23] while Mitchell advocated a mostly tactical air force that would perform defensive and offensive aerial roles (he proposed four branches of aviation: Pursuit, Bombardment, Attack, and Observation), along with precision tactical bombing of military and war-making facilities. [45] To that end, General Mitchell was determined to demonstrate to congress that Airpower

alone, left unchecked, could decide the outcomes of battles, and possibly wars, in the other two known domains. He was going to prove his statement of 1919, that “Only an air force can fight air force. Only an air force can keep ships afloat in war.” [9] He was going to prove that battleships without air protection could be sunk by airplanes alone.

General Mitchell made a request to the Appropriations Committee to use German ships for his demonstrations. These ships had been acquired through the treaties of WWI and were scheduled for destruction. [34] The Appropriations Committee agreed to hold a hearing on February 20, 1921 in which General Mitchell would state his case. Before General Mitchell was called to speak, several officials from the Army and Navy testified as to how useless airplanes would be against ships at sea, but when Billy Mitchell was called to the stand he caused a ripple of excitement throughout the room by stating: “We can tell you definitely now that we can either destroy or sink any ship in existence today.” [44] Of course, there had been no tests and he was not at all sure that it could be done, but he was willing to stake his career and reputation on the fact in order to be given the chance to try and prove his ideas correct. The Chairman then asked him if he really believed that, to which General Mitchell replied “Yes, sir, absolutely. All we want is to have you gentlemen watch us attack a battleship.” [44] The Chairman then asked him if the Navy also considered the tests important to national security, to which he replied “I cannot answer for them. Their whole training is that the armored ship is the mistress of the sea. Whereas actually it is just as helpless as was once the proud armored knight on horseback when gunfire first was brought against him.” [44]

The Appropriations Committee subsequently granted General Mitchell’s request to use several of the German ships for his aerial bombardment tests. One of these was the battleship *Ostfriesland*, the finest the German Navy had at the end of the war. A bombsight and some

2,000-pound bombs were then developed, along with theories based on the “water hammer” which dictated that bombs should explode underwater just off the side of a ship for maximum effect. [34] The tests were carried out, and on July 21, 1921, the *Ostfriesland* was sunk just as Mitchell expected. General Williams, Chief of ordinance, was heard to say: “A bomb was fired today which will be heard around the world.” [34] Billy Mitchell’s ideas were proved correct, and would eventually help to usher in a new chapter to modern warfare.

In the meantime however, Congress would choose not to act upon General Mitchell’s recommendations despite his best efforts, and American aviation would continue to flounder for another 20 years. During the Interwar Years, the Army retained control of aviation in the form of the Army Air Corps, but the corps was undermanned and not well funded. More than 15,000 flying officers trained during WWI had been dismissed from the Air Service to return to their civilian lives, and air power was not viewed as a priority to national defense. [45]

Conditions were ripe for disaster, until eventually the inevitable happened. On December the 7<sup>th</sup>, 1941 six Japanese aircraft carriers launched 351 airplanes in a sneak attack against the Pacific Fleet at Pearl Harbor. During the attack, 21 ships of the Pacific Fleet were sunk or damaged, 347 airplanes were destroyed or damaged, and 2,403 Americans were killed. Only 29 Japanese planes—less than 10%—were lost. The attack was a massive blow to the America’s national psyche and its military power in the Pacific theater. The oceans could no longer protect the heartland. [19]

At the time just before the United States entered WWII, the newly designated US Army Air Forces (USAAF) consisted of approximately 23,000 officers and men, only 2,500 of whom were rated pilots, and about 1,200 mostly obsolete combat aircraft—a force which lagged behind all the major world powers in the number and quality of its aircraft. The attack at Pearl Harbor

demonstrated what uncontested air power could do, and Major General Henry “Hap” Arnold, began building up the USAAF in earnest. Within five years after the US entered the war on December 8, 1941, the USAAF’s strength expanded significantly to 2.4 million troops and 70,000 planes. [6] Obviously, air power was now a military and national priority.

Throughout the remainder of WWII, General Arnold had been quietly laying the framework for an independent, strategic-minded air force. During the Interwar years, the War Department had generally viewed air power as a tool for defense and ground support operations. Air power theorists such as Hap Arnold, Billy Mitchell, and Ira Eaker believed that heavy, long range strategic bombers could be used (along with fighter escorts) alone to determine the course of war. Their theory was largely based on high-altitude strategic daylight bombing, but the theory was unproven. The Air Corps and General Arnold fought unsuccessfully for several years to get a portion of the Army’s small budget allocated for purchasing some Boeing B-17 bombers for this purpose, but they were continually stymied. As General MacArthur stated in one of his annual reports: “So far as tactical and strategic doctrine is concerned, there exist two great fields of Air Force employment; one fully demonstrated and proved, the other conjectural.” [53] In his mind, ground support had been “proved,” while strategic bombing and other air power theories had not. Eventually however, with war in Europe looming and President Franklin D. Roosevelt’s belief that “airplanes were the war implements that would have an influence on Hitler’s activities,” [53] Congress eventually approved the expansion of the air arm in 1939. Included within the expansion were over 100 of the new four-engine bombers. [53]

When war began, Arnold was promoted to lieutenant general and became a member of the U.S. Joint Chiefs of Staff and the Anglo-American Combined Chiefs of Staff. This was implicit recognition that the air force was equal to and independent of sea and land forces. This

move also matched the British staffing pattern and would ensure that Arnold's views were not filtered through an Army (i.e., ground force) bias. [6] Arnold made good use of his position, always politicking with other high ranking military and political officials. Three weeks after Germany invaded Russia, President Roosevelt requested estimates of the "overall production requirements needed to defeat our potential enemies." Arnold advocated that the Air War Plans Division (AWPD) be allowed to prepare its own annex to the War Plans Division's document. The AWPD developed AWPD-1, which was nothing less than a plan for defeating Germany by means of aerial bombardment alone. General George C. Marshall, War Department Chief of Staff, decided the plan had merit, and the spirit of the plan was approved at the Anglo-American conference in Washington in December, 1941. There is debate whether the war would have been won by air power alone, but subsequent bombing raids on Axis centers of gravity such as the oil refineries at Ploesti, the ball-bearing factory at Schweinfurt, and the U-boat yards at Wilhelmshaven would prove the importance of strategic air power in warfare. [53]

Throughout WWII, the increasing importance of a strong air arm reasserted itself time and again. In March 1942, the War Department issued Circular 59, *War Department Reorganization*, which was based largely on recommendations from General Arnold and which reorganized the Army into three autonomous commands: the Army Air Forces (AAF), Army Ground Forces (AGF), and the Army Service Forces (ASF). [53] Field Manual (FM) 100-20, *Command and Employment of Air Power*, was released in July of 1943. This document stated unequivocally that land power and air power were coequal and that the gaining of air superiority was the first requirement for the success of any major land operation. It went on to say:

*The inherent flexibility of air power is its greatest asset. This flexibility makes it possible to employ the whole weight of available air power against selected areas in turn; such concentrated use of the air striking force is a battle-winning factor of the first importance. Control of available air power must be centralized and command must be*



*exercised through the Air Force commander if this inherent flexibility and ability to deliver a decisive blow are to be fully exploited. Therefore, the command of air and ground forces in a theater of operations will be vested in the superior commander charged with the actual conduct of operations in the theater, who will exercise command of air forces through the air force commander and command of ground forces through the ground force commander. [83]*

Finally, Japan's capitulation and unconditional surrender after both the battle of Midway and the dropping of nuclear bombs over Hiroshima and Nagasaki unequivocally demonstrated in a dramatic fashion that air power could be decisive. The combination of these factors—the development of air warfare theory and strategy by pioneers such as Billy Mitchell and Giulio Douhet, advances in technology (bombers, fighters, bombs), skillful advocacy and politicking for resources by Hap Arnold, and demonstrated successes during WWII—ultimately resulted in the creation of a separate military service for fighting in the air domain. President Harry S. Truman signed the National Security Act of 1947, which established three military service departments (Army, Navy, and Air Force), under a consolidated Department of Defense (DoD). Truman had earlier stated: “Air power has been developed to a point where its responsibilities are equal to those of land and sea power, and its contribution to our strategic planning is as great. Parity for air power can be achieved in one department or in three, but not in two. As between one department and three, the former is infinitely preferred.” [6] The National Security Act became effective September 18, 1947—the US Air Force was finally born.

### **...and Space**

It would take another 10 years after the birth of the Air Force (54 years after the technology was invented that made possible the dominion of the air) before another new environment would emerge as a possible candidate for a warfighting domain. On October 4, 1957, the Soviet Union successfully launched the first man-made satellite, Sputnik I, into orbit around the earth. [54] It was a spectacular technological achievement and spurred the US into

action to quickly develop space technology of its own. Tensions of the Cold War and intercontinental ballistic missile (ICBM) threats were already high as the US and Soviet Union entered into a space race which would rapidly expand.

However, because of the extreme expense and difficulty of putting an object into orbit and the technical complexity of orbital mechanics, maneuver, and targeting, both the Eisenhower and Kennedy administration wished to avoid an arms race in space. Giulio Douhet's earlier quotation of "...wherever two men meet, conflict is inevitable" was not to hold true for Space in a literal sense. While it is true that earthly conflicts have occurred over the use of space, there have been no actual conflicts within space itself. As noted in the 1958 law creating the National Aeronautics and Space Administration (NASA), "The Congress declares that it is the policy of the United States that activities in space should be devoted to peaceful purposes for the benefit of mankind." [6] This includes transnational overflights for spacecraft in orbit.

The Eisenhower Administration believed that "peaceful purposes" included national defense support missions such as reconnaissance and communications. The DoD was given the responsibility for developing and operating these defensive systems in space. DoD Directive 5160.22 (September 1, 1970) subsequently declared that "the Air Force will have the responsibility of development, production, and deployment of space systems for warning and surveillance of enemy nuclear capabilities, and all launch vehicles, including launch and orbital support operations." [6]

Over the next decade, the Cold War space race between the US and USSR escalated dramatically—the Soviets launched nearly 100 satellites in 1981. This resulted in an increased interest in the creation of space doctrine and the establishment of a space organization. These calls, along with the Reagan administration's build up of the military, the rapid growth of space

technology and advanced satellites (military and commercial), and the development of the Space Shuttle all set the stage for Air Force Chief of Staff General Lew Allen's June 21, 1982 announcement of the formation of Air Force Space Command, effective September 1, 1983. [6]

By now the parallels between the development of air and space organizations and professionals should be evident. In each case, technology was developed to operate in and exploit the air/space environment; theory and doctrine for employing the technology to control the domain were then developed; and finally, an organization was created to provide advocacy and sustainment of the force.

The similarity ends there, however. The first commander of AFSPC, Gen. James V. Hartinger, was only half correct in his statement: "Space is a place... It is a theater of operations, and it was just a matter of time until we treated it as such." [61] Space is indeed an operational environment, a strategic high ground of sorts. However, we have not really treated it as a warfighting domain in the same sense as sea, land and air. While there has been talk of a separate branch of the military for space, there has been insufficient justification because the domain has largely been uncontested.

There are a couple of reasons why this is the case. First, nations have artificially limited their activities in the space environment, specifically prohibiting certain military activities. There are a number of international treaties and resolutions on the subject, such as the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies* (1967). Article II of this treaty specifically states:

*Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means .[1]*

While Article IV states:

*States Parties to the Treaty undertake not to place into orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.*

*The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the moon and other celestial bodies shall also not be prohibited. [1]*

The second reason Space is not a true warfighting domain is that there has not been—outside of testing and experiments—attempts to control space, at least in the same sense as in the other domains. Until there is sufficient threat—to include possible loss of life and/or space assets—it is difficult to argue for building up an offensive and defensive capability. This in turn limits our ability to develop tactics and doctrine for warfighting, because doctrine is a distillation of historical vignettes, case studies, and lessons learned. Short of experimenting and testing theories in practice, it is difficult to learn anything. Hap Arnold and others strongly believed in the need for a separate military service focused on the air domain, but it was only after airmen demonstrated their worth in WWII that the need for a separate air force received any traction. We have not yet had a similar experience in the space environment.

Joint Publication 3-14, *Joint Doctrine for Space Operations*, states the four primary mission areas in space thusly: “Within the domain of space operations, there are four primary mission areas: **space control, force enhancement, space support, and force application,**” described in more detail below:

***Space control** operations provide freedom of action in space for friendly forces while, when directed, denying it to an adversary, and include the broad aspect of protection of US and US allied space systems and negation of enemy adversary space systems.*

*Space control operations encompass all elements of the space defense mission and include offensive and defensive operations by friendly forces to gain and maintain space superiority and situational awareness if events impact space operations.*

***Space force enhancement** operations multiply joint force effectiveness by enhancing battlespace awareness and providing needed warfighter support. There are five force enhancement functions: **intelligence, surveillance, and reconnaissance; integrated tactical warning and attack assessment; environmental monitoring; communications; and position, velocity, time, and navigation.***

***Space support** operations consist of operations that launch, deploy, augment, maintain, sustain, replenish, deorbit, and recover space forces, including the command and control network configuration for space operations. Support operations consist of spacelift, satellite operations, and deorbiting and recovering space vehicles, if required.*

***Space force application** operations consist of attacks against terrestrial-based targets carried out by military weapons systems operating in or through space. **Currently, there are no space force application assets operating in space.** [77]*

Not all of these missions are currently practiced. Space control functions are generally limited to protective and defensive measures (to prefer our own ability to use the environment). As stated in the Joint Publication, there are no current capabilities regarding force application. Lt Col Martin E.B. France characterized these shortcomings well in his paper on the subject:

*Not only does the United States possess no comprehensive means of directly attacking an adversary's space forces on orbit, it also lacks any ability to actively defend its assets already on orbit from a surface-based or orbital attack. The result is an unprecedented amount of wealth representing overwhelming strategic value left undefended in space today, with the target date for fielding systems capable of protection and negation in space no sooner than 2020 by even the most optimistic forecast. While the distances and speeds involved make directly attacking our assets admittedly difficult, the possibility of a successful, limited attack using technology available to any spacefaring nation or even some limited to intermediate range ballistic missiles is real. The result is an assumed sense of space superiority that exists if for no other reason than no successful, documented attacks on U.S. systems have yet occurred. [29]*

Given all of this, much of Space Command's role (at least to the extent that can be discussed here) is that of caretaker. It launches space vehicles and tracks their orbits, maintains ICBM's, watches for enemy launches, and monitors national airspace. Its one "space-as-a-

warfighting-domain” function is maneuvering of satellites into appropriate positions for intelligence, surveillance and reconnaissance (ISR) purposes.

Space law and treaties do leave open the possibility of conventional weapons platforms, national security assets, and self defense of space vehicles and equipment; however, no nations, including the United States, have yet to venture down this road with the exception of the aforementioned ISR satellites, which are in essence the space-equivalent of the observation balloons in the Civil War (albeit at a much greater height). If we continued to use the air environment for observation purposes, then it is highly unlikely that we would have an air force, let alone an air domain. It only becomes a domain when parties struggle for control of the environment. This is the current situation with space.

Given these two major constraints and the limited resources provided, Air Force Space Command admirably discharges its responsibilities. Eventually, space may be more fully utilized as a warfighting domain, which would shift priorities and resource allocation accordingly. Until that happens, we will continue to use outer space primarily as a parking lot for communications, navigation, ISR and other purposes, which primarily support terrestrial operations.

### **Cyberspace Emerges.**

As is so often the case, history was soon to repeat itself in regards to another new domain. In the early 1940’s, J. Presper Eckert and John Mauchly were the “Wright Brothers” of their time in the fledgling field of computers. Whereas Orville and Wilber’s invention of the first powered aircraft made possible the exploitation of the air environment, John Eckert and John Mauchly’s invention was to make possible the exploitation of a new environment that would be created a scant only a few years after the first successful space launches—an

environment which would exist only within a network of machines. Eckert and Mauchly had invented the first all-electronic computer, dubbed the ENIAC or Electronic Numerical Integrator and Computer. [70] At that time, computers were merely tools; they were able to increase humanity's quality of life by doing complex calculations and storing information for easy retrieval, but could not directly affect human's lives. Although the invention of the computer brought forth the tool necessary to exert dominion over an environment much as the airplane did for Air in 1903, the comparison ends there with the fact that the environment that the computer would exploit *did not yet exist*. It would take the invention of computer networking in the late 60's and early 70's to bring the new environment into existence.

In 1962, the US Air Force commissioned a RAND Corporation study on how it could maintain positive command and control over strategic missiles and bombers after a nuclear attack. RAND's final proposal was a packet switched network, which ultimately laid the groundwork for the Advanced Research Projects Agency Network (ARPANET). The ARPANET contract was awarded in 1968 to a company called BBN out of Massachusetts, who completed construction of a 50 Kbps network between the University of California at Los Angeles, Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah in 1969. [37] Cyberspace was born.

In 1973, the unreliability of the first network protocol and the growing number of hosts (now over 23!) prompted the Defense Advanced Research Projects Agency (DARPA) to begin development of a new transmission and routing protocol which would come to be known as TCP/IP. TCP/IP was really two protocols—TCP (transmission control protocol) provided for flow control and assured delivery, whereas the internet protocol (IP) provided for addressing the network nodes and routing of traffic through the network. Three years later, the DoD mandated

the use of TCP/IP for all hosts connected to ARPANET by January 1<sup>st</sup>, 1983. In 1981, the National Science Foundation created their own backbone, called CSNET for use by people who did not have access to ARPANET and proposed a plan for an interconnection between the two networks. In 1983, the University of Wisconsin created the Domain Name Service, or DNS. DNS was an important step in that it provided a quick way of translating between human readable addresses (e.g., www.msn.com) to machine readable addresses (e.g., 65.54.152.126). Over the next decade, many new network technologies were developed, but they were primarily limited to universities, research laboratories, and military agencies. In 1992, the World Wide Web was introduced by CERN (European Organization for Nuclear Research), and Delphi began offering commercial internet subscriber service. In 1993 InterNIC was created by the National Science Foundation to provide internet services through three vendors: AT&T, Network Solutions Inc., and General Atomics/CERFNet. In 1995, all pretenses to the limitation of commercial use disappeared when the NSF ended its sponsorship of the internet backbone—America Online, Prodigy, and CompuServe (among others) quickly moved into the fray to offer their own internet services. From the time the internet went commercial in 1992 to the time the NSF officially ended its sponsorship of the backbone (just four years), the amount of hosts connected to the internet jumped from 1.1 million to 6.6 million. [37]

The internet spread to all corners of the world, growing at an exponential rate. There are now approximately 500,000,000 hosts connected to the internet, which are located in every country in the world. [33] Along with massive growth came an increasingly heavy reliance upon cyberspace for the more technologically advanced nations. Paper records were eschewed in favor of electronic storage and retrieval over computer networks (i.e., the “paperless office”), supervisory control and data acquisition (SCADA) systems were networked to facilitate remote



control of industrial processes, online banking and commerce became the norm, communications were increasingly routed over packet switched networks, and unmanned vehicles were controlled with radio frequency signals. With this plethora of information, control, and wealth reachable from across the internet came exponentially increasing vulnerabilities to attacks from individuals, organized crime syndicates, and even nation-states seeking to steal, destroy, modify, or disrupt the flow of information. In short, cyberspace has become a center of gravity for our nation and many others; further, it is a contested environment in which people and organizations are attempting to control, deny, or restrict our own ability to use and exploit the environment—in other words, cyberspace is a domain, just like air, land and sea.

As such a need was recognized to be able to hold another's cyberspace capabilities at risk while defending our own. On December 5<sup>th</sup>, 2005 the Air Force declared that Cyberspace was an operational domain in which it would fly and fight. Former Secretary of the Air Force Michael W. Wynne confirmed the risks and justified the new domain by stating: "What we are seeing is that the Cyberspace Domain contains the same seeds for criminal, pirate, transnational, and government-sponsored mischief as we have contended within the Domains of Land, Sea, Air, and now contemplate as Space continues to mature." [85]

Up to this point, authorities on the doctrinal subjects of warfare have tried to link each Operational Domain to a naturally occurring environment. In the case of Cyber, these authorities attempt to tie said domain to the electromagnetic "environment," and later to an information "environment." [73, 26] However, neither electromagnetism nor information can be environments. Electromagnetic terrain and objects, and therefore battlefields and targets, cannot exist without human intervention and creation. Electromagnetism is a force of physics, and while many tools exist which make use of and manipulate the electromagnetic spectrum, it is not

possible for an environment to exist as a subset of a force. If it were, we would have to consider gravity as an environment.

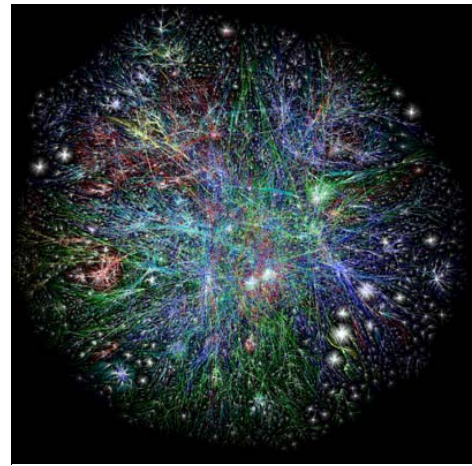
Similarly, information is not an environment—information is a noun, a thing. Electromagnetic representations of information may reside within a man-made environment, but it cannot be an environment in and of itself. Information can be the objective of an attack (stealing, denying access to, corrupting, etc.), but is not itself the field over which the attack traveled to its objective. Dominion cannot be contested over information; only the machines and infrastructure it resides upon and travels through. The DoD tries to sort this out by giving the “information environment” its own definition: “The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.” [76] But this definition singles out the entities of an information environment as individual and separate, whereas an environment should be a contiguous, all-encompassing thing. It gives no mention to the man-made infrastructure which ties it all together, interconnectedness being one of the necessary trademarks of cyberspace. Additionally, cyberspace would not be able to map directly to this “information environment” because human beings and organizations are included within it. Dominion may not be contested in cyberspace over individuals or organizations; only systems, and even then only systems of machines.

Some will no doubt be asking “If that’s the case, then what environment encompasses the cyberspace domain?” It is the author’s opinion that cyberspace is not natural but is man-made...call it *machine*.

*...while the physical characteristics of cyberspace can be delineated and come from forces that exist naturally in the physical world, in a very real sense cyberspace is a designed environment, created with the very specific intent of facilitating the use and exploitation of information, human interaction and intercommunication.*

*-Dr. Dan Kuehl, National Defense University*

The machine environment was not always possible. It was only through the interconnectedness and “awareness” of machines to their electromagnetic networks and the systems they were connected to that it became possible. Notice I said “awareness” and not “self-awareness,” although this too may likely become possible in time. It is an important distinction to make – once machines can think for themselves, it may no longer be an environment we can control. The world of SkyNet in the *Terminator* movies may sound like science fiction, but then so did most modern technologies in times past. [52] Modern computers and micro-processors are unique in the fact that they can be either tools *or* a component of the machine environment, or even both at the same time. When disconnected from a network, a computer is a tool; you can use it for word processing, doing sums, etc. When plugged into a network, it instantly becomes part of the machine environmental landscape and can threaten your interests as easily as it can help them. This holds true for *any* computerized machine connected to a network. For example: an unmanned aerial vehicle, a communications satellite, or even a cellular telephone is also part of the machine landscape. In a traditional sense, these devices are targets—such as a tank or a command and control facility. But these devices are also *terrain* that is contested—we strive to protect and defend our cyberspace assets in the same way that ground and naval forces seize and hold key terrain and choke points. Once again turning to science fiction for an example, we see that the humans of *Battlestar Galactica* are wary to the extreme of networking any computer in the fear that the Cylons will then be able to use their once-tools against them. [49]



**Figure 2 - The Machine Environment (Cyberspace). [87]**

Although computers are electronic machines which make use of the electromagnetic spectrum, there are other types in development which are not, particularly in the nano and bio-mechanics fields. Rest assured that these new kinds of machines will also be somehow linked into the machine environment in order to facilitate remote control and increase usefulness.

This constant move towards ever-expanding amounts of control and utility is one of the trademarks of cyber development; operations within and dependence upon cyberspace have steadily grown over the years since 1969. However, as the cyberspace domain has increasingly become a contested territory, it is being made clear that the capacity for defense has not kept pace with the capacity to attack. It is only recently that we have seriously begun to treat cyberspace as a warfighting domain. In keeping with the previous discussions on air and space, this will include developing cyberspace operations theory and doctrine (who is the cyber-equivalent to Billy Mitchell?), as well as organizing, training and equipping a cyber force. Hopefully we can make serious progress in these areas before our increasingly cyber-dependent national interests are threatened with an electronic “Pearl Harbor” attack with strategic consequences. The cyber attacks on Estonia in April and May of 2007 in which 20,000 networks of compromised computers were linked up to cripple the country’s financial and governmental offices and the well-coordinated Russian recruitment of an international cyber-militia to attack Georgia in 2008 were but a very small taste of such a surprise attack. [43, 36] Distributed Denial of Service (DDoS) attacks and web defacements as were seen in Estonia, the more sophisticated yet still non-destructive web server attacks that were seen in Georgia, or disruptions caused by virus replication as was seen with the Code Red, Blaster, and Slammer variants in 2001 and 2003 are nothing compared to the widespread and debilitating damage that would be caused by a virus with a destructive payload.

As with the air domain, other countries are moving ahead in developing capabilities for exploiting and controlling the machine environment. Cyberspace is clearly a domain in which the US (and the rest of the Western world) has peer and near-peer competitors. [15] Chinese military thinkers have specifically begun theorizing and developing doctrine for integrating cyber warfare capabilities with other elements of national power, as evidenced by the concept of “informationization” (xinxihua) put forward in China’s 2006 white paper on national defense. [30] Foreign ideas, strategies, and doctrine are in advance of our own in large part because our top officials in the Army, Navy, and Air Force are thinking in terms of the past, most comfortable with doing things the way they’ve always been done. [8] If there is one thing history has taught us, it is that our armed forces are slow to change. Compounding this fact are budgetary concerns in Congress: if they do not see a clear and present danger, they may not wish to spend billions of dollars as a response to an unspecified, vague threat. Just as in the time of Billy Mitchell, it might take an astonishing demonstration, a Cyber “sinking of the *Ostfriesland*” to prove that the juggernauts of the 21<sup>st</sup> century are, as General Mitchell put it, “as helpless as was once the proud armored knight on horseback when gunfire first was brought against him” [44] in regards to cyber operations. One would think that an exercise consisting of a no-holds-barred unleashing of cyber capabilities against our nation’s infrastructure would jolt the nation’s leaders into action. However, in 1997 and again in 2003, the Department of Defense-run Operation Eligible Receiver – an effort to test the vulnerability of this nation to electronic attack – failed to catch the attention of Congress. According to an account published in the Washington Times, “Senior Pentagon leaders were stunned by a military exercise showing how easy it is for hackers to cripple U.S. military and civilian computer networks.” [48] In a few days and using only commercial-off-the-shelf computer equipment, the red team hackers had infiltrated the computer systems controlling parts of the nation’s electric power grid and with a series of commands could

have turned sections of the country dark. “If the exercise had been real,” the Christian Science Monitor reported, “they could have disrupted the Department of Defense’s communication systems (taking out most of the Pacific Command) and gained access to computer systems aboard U.S. Navy vessels.” [48] Sadly, a demonstration on a financial institution may have been a better showcase, as threats to the nation’s pocketbook seem to generate more dismay than threats to the nation’s military that could be alleviated by more defense spending.

The difficulties with advancing the cause of cyberspace and cyber power are similar to those experienced in the early 1900’s: cyberspace is largely seen as a supporting domain for other missions, and we have not had a well-defined career path for developing cyberspace professionals, to include appropriate leadership positions—at least not to the same extent as we develop air and space leaders. As to the first point, it is clear that each service is concerned with protecting its own portion of cyberspace—because they have to protect their ability to operate in their primary domains. Each service has begun efforts to formally develop cyberspace capabilities. In 2006, the Air Force embarked on a plan to create a new major command specifically for organizing, training and equipping a cyber force. In a “Go-Do” letter to 8<sup>th</sup> Air Force Commander, then-Chief of Staff of the Air Force General T. Michael Moseley wrote that his intent was to “redefine airpower by extending the Air Force’s global vigilance, global reach, and global power into the cyberspace domain” by directing Eighth Air Force “to leverage, consolidate, and integrate Air Force unique cyberspace capabilities and functions... across the spectrum of conflict.” [50] A provisional command, AFCYBER(P), was subsequently activated in 2007, with a permanent major command activating in October 2008. The mission of AFCYBER was to “provide combat-ready forces trained and equipped to conduct sustained combat operations in and through the electromagnetic spectrum, fully integrated with air and space operations.” [67] Major General William T. Lord, AFCYBER(P) Commander, stated

“Controlling cyberspace is the prerequisite to effective operations across all strategic and operational domains—securing freedom from attack and freedom to attack.” [67] The Air Force has since backed off on creating a separate major command for cyberspace, and has decided to create a cyber-focused numbered air force under Air Force Space Command. This move does not mean that cyberspace is no longer viewed as important, but rather reflects fiscal and resource constraints.

A common theme in the quoted statements above is that the Air Force seems to be—to paraphrase Billy Mitchell’s words—“thinking first of airplanes, and making cybercraft secondary to that.” The Army and Navy are also developing their own cyberspace capabilities, and their activities will no doubt be focused on their primary domains (land and sea) and how cyberspace supports them. This is only natural and expected, since the development of cyberspace specific capabilities will be competing for scarce resources against existing warfighting requirements.

A natural question, however, is who in the DoD is (or should be) looking specifically at warfighting in the cyberspace domain and defense of the nation in cyberspace, to include government, private sector, and academia. It is the author’s contention that cyberspace will likely not receive the level of attention and advocacy it needs until a new service is created specifically for the domain—because the existing services will be focused on their primary domains. Unfortunately, it may take a significant event (equivalent to launch of the Sputnik or sinking of the *Ostfriesland*) to galvanize activities. The Comprehensive National Cybersecurity Initiative (CNCI) released in early 2008 and ongoing Quadrennial Defense Review will no doubt be focusing on such issues.

To summarize, cyberspace has overtaken space and is now a warfighting domain in every sense. Hundreds of thousands of probes and attacks occur in cyberspace every day. Space is largely demilitarized (for various reasons) and is similar to the “observation balloon” stage of air exploitation, whereas cyberspace has advanced to the “WWI prop fighter” and Interwar period, with another Pearl Harbor looming over any unwary nation. Dominion is being contested on a daily basis. The United States needs to formulate the strategy, the doctrine, and the force to protect our cyber homeland while working towards the “cyber advanced multi-role stealth fighter-bombers” before another country develops a “cyber nuclear bomb.”



### III. The Nature of Power and Dominion

#### What is (Military) Power?

*War is nothing but the continuation of policy with other means.*

*-Carl von Clausewitz*

*The strategist is he who always keeps the objective of the war in sight and the objective of the war is never military and is always political.*

*-Alfred Thayer Mahan*

Over the centuries, all civilizations have attempted to utilize force of arms in order to afford themselves more power relative to various other external entities. The reasons for this are many and complex, but the National Military Strategy for the United States distills them down to just three: protect the nation against external attacks and aggression, prevent conflict and surprise attack, and prevail against adversaries. [79] Each branch of the military is then responsible for organizing, training, and equipping forces to Combatant Commanders (warfighters). It is left to the individual services to formulate the means of generating power in their individual domain given the tools that are available to them and then applying that power (with the additional input of the Joint Chiefs of Staff and the direction of the Combatant Commanders) to affect an adversary's centers of gravity (more on these in a bit). The relevant entries in Merriam-Webster's dictionary define power thusly:

**POW•ER** \ n

1. ability to act or produce an effect.
2. possession of control, authority, or influence over others.
3. physical might. [59]

Indeed, the military's overarching goal is to gain and maintain its ability to act or produce effects through physical (kinetic) and non-physical methods in order to exert control and influence over others. But where do nations derive this power, and how should this power be applied for maximal effect to cause capitulation to your demands? The answer to the first question has been

put forth by the formulation of the Instruments of National Power, which are commonly accepted to be Diplomatic, Informational, Military, and Economic (DIME), but have been recently expanded to include financial systems, intelligence, and law enforcement (DIMEFIL). [27] The focus of this research is on the Military instrument (to include cyber), although it may well touch upon other instruments where they overlap (most notably the Informational, Economic, Financial, and Intelligence instruments). The answer to the second question—how should power be applied?—has been studied extensively by military theorists, among them Carl von Clausewitz, Alfred Thayer Mahan, and John Warden. A common theme discussed throughout the literature is the concept of “Center of Gravity” (CoG). [12]

Clausewitz defined a center of gravity as “the hub of all power and movement, on which everything depends.” [12] Modern US military doctrine has redefined centers of gravity as “those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight” [62], as those “characteristics, capabilities or locations from which a military force derives its freedom of action, physical strength, or will to fight” [75], and yet again and most recently as “a source of power that provides moral or physical strength, freedom of action, or will to act.” [78] Reasons for these frequent changes and re-definitions can perhaps be traced to a bad translation from the original German within the most popular edition of Clausewitz’s book, *On War*. Theorists have gone back to the original texts and noted that Clausewitz never used the word “source,” (*quelle*, in German) and that he was very enamored of the science of physics at the time of his writings. A Clausewitzian CoG is not a strength, nor is it a source of strength. Most likely to him, a center of gravity was the one element within a object’s entire structure or system that had the necessary centripetal force to hold that structure together. Additionally, because Clausewitz’s CoG focuses on achieving a

specific effect, the collapse of the enemy, it is an effects-based approach rather than a capabilities-based one and it resembles the concept of Effects-Based Operations (EBO). [25]

Furthermore, Clausewitz advocated attacking these centers of gravity with all the force possible. Some of his thoughts are summarized as follows: “war is an act of force, and there is no logical limit to the application of that force,” “the grand objective in all military action is to overthrow the enemy,” and “destruction of the enemy is what always matters most.” [12] This idea of centers of gravity and absolute war is very important to cyber power. Attacking targets in cyberspace does not necessarily kill people, although indirect 2<sup>nd</sup> and 3<sup>rd</sup> order effects may certainly result in physical destruction and loss of life. Nor will cyber attacks occupy and hold territory (at least in a physical sense). Using Clausewitz’ ideas, it would seem that cyber power would be brought to bear on one or more of the few centers of gravity that can be reached via cyberspace (e.g., financial; economic; and informational CoGs) with all possible effort. Further, the attacker must be prepared to detrimentally affect every living human being in the target country. As General Lord has stated, cyber power when used to win wars may be a weapon of mass disruption. [11] If any lesser effect than total collapse is desired (i.e., Clausewitz’ concept of a “limited war” or “war with limited aims”), cyber power may play a mere supporting role to attacks in the other domains. The 2007 report *Flying and Fighting in Cyberspace* backs this assertion:

*Cyber capabilities can assuredly support applications of other force capabilities, but, fundamentally, they are not the destructive, kinetic purveyors of violence that war fighters traditionally envision in planning military strategy, engagements and wars. If we apply them as primary weapons of war, then basic concepts regarding the use of force or threat of force to compel the enemy must change. [13]*

Adding more challenge than just the small number of possible categories from which to choose centers of gravity in cyberspace is the fact that conditions must be just right for a country to have any of them at all. For example, an informational CoG may be more meaningful in a country ripe for coup, revolution, or collapse due to shattering of ideologies or propaganda. Likewise, economic and financial CoG's do not exist except for countries or entities that rely heavily on cyberspace and are highly dependent upon a capitalistic-style economic furnace or

organizations that require movement of funds through numbered bank accounts.

**Table 1 - Actor Center of Gravity Dependence**

**Actor Center of Gravity Dependence**

Actor Category \ Cyber COG	Financial	Economic	Informational
Capitalistic Superpower	●	●	○
Communist Superpower	◐	◐	◑
Average Dictatorship	◐	○	◑
Average Democracy	●	◐	○
Terrorist Organization	◐	○	●
Drug Cartel	●	○	○
Third World	○	○	○

○ = Little to no dependance    ◐ = Moderate dependance    ● = Heavy dependance

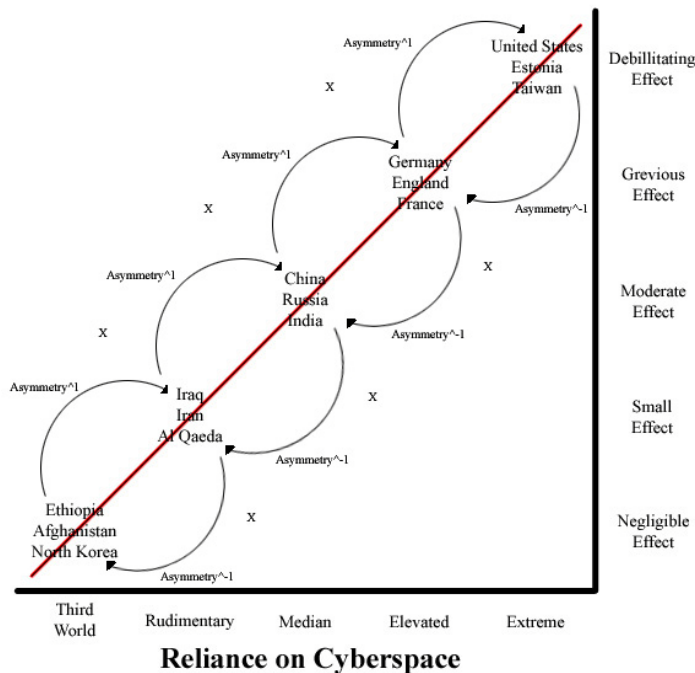
This is illustrated in the chart at left, in which certain actors are more reliant upon certain cyber CoGs than others. For example, in a capitalistic superpower such as the United States, an attack on financial and economic CoGs could have a great effect, whereas an informational attack would be shrugged off. Disinformation, psychological operations, or propaganda may cause a certain amount of distrust, but would probably not cause an insurrection or

coup, the government having a long history of providing for its people. In a more authoritarian society, the informational CoG gains more importance. For example, the People's Republic of China has an extensive Internet censorship program to restrict the flow of information among its citizens to those topics that have been deemed "acceptable" by national leaders. On the other

hand, the economic CoG may lose some importance because China is largely an industrial/agricultural country that can produce many of its own goods, and its financial CoG also loses some importance because in a communist society laborers will work “for the good of the people” with little or no compensation. Lastly, in a terrorist organization, the financial CoG has moderate importance. Funds from numbered bank accounts are disbursed to finance terrorist cells in many diverse countries. However, Al Qaeda would still be able to carry out limited attacks with no funds, as it also uses religious extremism to garner operatives to its banner. The economic CoG has no bearing on a terrorist organization because they do not trade with anyone or produce anything, but the informational CoG is highly important because it is through ideology and propaganda that they derive their power.

Along with the relative importance of Cyber CoGs to individual actors, another chart can be used to estimate the effects of an absolute war in cyberspace. This chart shows the relative

**Table 2 - Asymmetric Effects of Cyber Warfare**



damage that could be caused based upon a target’s reliance on cyberspace. Many third world countries have little or no reliance on cyberspace, and therefore a cyber attack on them would have negligible effect. Countries like China, Russia, and India have small pockets of advanced information

technology, but large percentages (91.5% in the case of China) of their very large populations are in rural areas with very limited access to (or need for) cyberspace. [60] An attack on a cyber CoG in countries such as those would cause disruption, but ultimately might not create enough damage to the nation as a whole to cause capitulation. Finally, highly advanced—i.e., “wired”—countries such as the United States, Estonia, and Taiwan, are almost totally reliant on cyberspace, and as such attacking a cyber CoG of great importance would almost certainly cause a great amount of disruption, as was seen with the example of Estonia in 2005.

Putting the two charts together, we can see that attacking a cyber CoG of great importance in a country with high reliance on cyberspace could create a debilitating effect. Attacking a cyber CoG of moderate importance to a country would cause an effect that was one step lower than on the “Effects of Cyber Warfare” scale, and attacking a CoG of little to no importance would create an effect two steps lower. It is interesting to note that this graph also depicts the relative asymmetry of cyber attacks. A third world country could attack an extremely advanced nation, yet any tit-for-tat reprisals have limited utility. Additionally, one can also think of these relative orders of magnitude in terms of cost of infrastructure, maintenance, technicians, research and development, engineers and scientists required to effectively operate and provide for defense in cyberspace. For example, North Korea’s investments in establishing and defending its cyberspace infrastructure are much less than those required by, say, Taiwan. This does not hold true for an attack capability, as this capability can come very cheaply in the form of inexpensive second-hand laptops and downloaded script-kiddy attacks.

In order to effectively attack and destroy centers of gravity, modern war planners and strategy theorists generally recognize nine principles of war which apply (although not equally) to all domains of warfare. These principles have grown out of and been influenced by all the

great military thinkers, but most influential among them is Clausewitz. Many of these principles are included in his seminal work, *On War*, as incontrovertible points of strategy. Examples are boldness, perseverance, superiority of numbers, surprise, cunning, concentration of forces in space, unification of forces in time, strategic reserve, and economy of force. [12] The U.S. Army adapted these principles and published them in their “Operations” field manual (FM 3-0) as the Principles of War: objective, offensive, economy of force, mass, maneuver, unity of command, simplicity, surprise, and security. [69]

- *Objective* is described as “direct[ing] every military operation toward a clearly defined, decisive, and attainable objective.” [69] While not explicitly defined in Clausewitz’s points on strategy, objective is a strong thread that runs through his writings in regards to centers of gravity, which he believed of utmost importance to the winning of wars. [12]
- *Offensive* means to “seize, retain, and exploit the initiative,” and is synonymous with boldness. [69]
- *Economy of Force* is taken unchanged, and is defined by the Army as “allocat[ing] minimum essential combat power to secondary efforts.” [69]
- *Mass* means to “concentrate the effects of combat power at the decisive place and time,” and correlates with Clausewitz’ principle of concentration of forces in space and unification of forces in time. [69]
- *Maneuver* means to “place the enemy in a disadvantageous position through the flexible application of combat power,” [69] and while not one of Clausewitz’s points of strategy, he did think it important enough to get its own chapter later in his book.

- *Unity of Command* is the belief that an army should, “for every objective, ensure unity of effort under one responsible commander.” [69] This point was also not explicitly addressed by Clausewitz, although there are undercurrents of this idea throughout his writings.
- *Simplicity* is explained as “prepar[ing] clear, uncomplicated plans and clear, concise orders to ensure thorough understanding.” [69] Again, this was not part of Clausewitz’s strategic points, but it is a theme which recurs quite frequently throughout the rest of his writings: “everything in war is very simple, but the simplest thing is difficult.” [12]
- *Surprise* is to “strike the enemy at a time or place or in a manner for which he is unprepared,” [69] and remains unchanged from Clausewitz’s original point.
- And finally, *security* is to “never permit the enemy to acquire an unexpected advantage,” [69] which maps directly to Clausewitz’s “cunning” point of strategy.

We see that of Clausewitz’s nine original points, the Army kept six of them (consolidating two into one in one case), and added four not specifically mentioned in Clausewitz’s “On Strategy in General” chapter but were nonetheless important themes throughout the rest of his work. Three strategic points dropped by the Army (perseverance, superiority of numbers, and strategic reserve) were deemed as either going without saying (as in the case of perseverance and strategic reserve), or outmoded by technology (superiority of numbers). While these are the widely accepted principles, some of the ways that each branch of service goes about practicing them necessarily differ quite widely based upon the specialized environments in which they operate. Additionally, some principles may have more importance in a certain domain and less in another. Let us now look at each domain individually.



## Theories of Military Power

When conversing about military power, there are certain individuals whose names spring to mind and who are generally regarded as the subject matter experts in relation to the domains they studied. For the land, environment, the writings of Sun Tzu, Antoine-Henri Jomini, and Carl von Clausewitz are prominent. For contests at Sea, Alfred Thayer Mahan and Julian S. Corbett were the visionaries whose writings still greatly influence our navy today. As discussed earlier, Giulio Douhet and Billy Mitchell were the leading pioneers of the air domain, followed more recently by people like John Boyd and John Warden. There have been some attempts to codify doctrine and space power theory such as David E. Lupton's 1998 work On Space Warfare, but as has been discussed earlier, the non-militarization of space has limited space as more of a supporting environment rather than a warfighting domain. Given the embryonic state of cyberspace as a warfighting domain, there are no real Billy Mitchells, but this will change as we learn more about applying power to achieve effects in the domain. Cyber power can be related to power in each of the other domains by varying degrees, as will be discussed in the following sections.

### Power on Land

*[Y]ou may fly over a land forever; you may bomb it, atomize it, pulverize it and wipe it clean of life—but if you desire to defend it, protect it, and keep it for civilization, you must do this on the ground, the way the Roman legions did, by putting your young men into the mud.*

-T. R. Fehrenbach [69]

Land warfare is the oldest and perhaps most understood of all the fighting disciplines; however, it is also the least analogous to cyber power. Terrain and weather don't matter, maneuver is somewhat meaningless, and a direct approach works better than an indirect. The one way in which cyber power does resemble power on land concerns its use to influence a

nation's center of gravity. Over the centuries, certain technological advances have altered aspects of military power on land, but the basic concepts remain the same. Sun Tzu was the first military theorist whose written works survived through the ages. In his book *The Art of War*, written in China 2,500 years ago, he wrote very generally about the derivation and grand strategy of land power, stating only that "War is a matter of vital importance to the state; the province of life or death; the road to survival or ruin." [62] When describing importance of targets (Sun Tzu's centers of gravity) and how power should be applied to these targets, he wrote: "...The best policy is to take a state intact; to ruin it is inferior to this. To capture the enemy's army is better than to destroy it... to subdue the enemy without fighting is the acme of skill. Thus... of supreme importance in war is to attack the enemy's strategy; the next best is to disrupt his alliances; the next best is to attack his army; and the worst policy is to attack cities." [62] What Sun Tzu did write extensively about was doctrine and tactics – the employment of land power. According to him, there are five fundamental factors which shape power on land. Those are: moral influence, weather, terrain, command, and doctrine (do not confuse the modern definition of this word with Sun Tzu's use of it).

- Moral influence: Sun Tzu was speaking of the extent to which the people of a nation or army were in harmony with its leadership; the will to fight. [62] This is important to any conflict, including those in cyberspace. However, it is less important on the digital battlefield as there is a greater willingness to press a button or type a few keystrokes than there is to place yourself bodily into the line of fire to be killed or maimed. This extends to a nation's populace; the United States would be more likely to engage in a cyber war, as it bears no immediate (physical) risk to the nation's sons

and daughters (although the saying “those who live in glass houses shouldn’t throw stones” comes to mind).

- **Weather:** By this, Sun Tzu meant that the natural forces of snow, rain, heat, etc., would greatly affect the power which could be brought to bear in combat. [62] In those days, such things could easily kill or wear down a large percentage of your army in the field before ever engaging with the enemy. In terms of cyberspace, weather is much less a factor than in other domains. With the exceptions of a lightning strike taking out a critical router, rain shorting out a badly insulated wire, or adverse environmental conditions such as sun spots or atmospheric scatter due to cloud cover affecting satellite or radio frequency propagation, the weather plays a very small role in cyberspace operations.
- **Terrain:** Sun Tzu included distance, ease of traversal, favorability of maneuver, and inhospitable features into this category. [62] Again, this is a factor which bears limited corollaries to the cyber landscape. Although there are network topologies to consider when planning both attacks and defenses, travel to critical nodes is not influenced by features of the cyber landscape. Distance is traversed in milliseconds at near the speed of light, propagation of signals occurs just as well (or well enough as to make no difference) along their path, and maneuver is somewhat meaningless (as a signal will travel to an enemy’s fixed IP along any path available) except in making attribution more difficult.
- **Command:** Sun Tzu meant the qualities of leadership including wisdom, sincerity, humanity, courage, and strictness. [62] Leadership is a factor influencing power in all domains. In cyberspace just as on the ground, bad leaders will not recognize

changing circumstances and act expediently, nor will they encourage creativity or ingenuity of troops, and they will also not seize opportunities when they arise. It is leadership who assumes the risk in decisions of defense and attack.

- Doctrine: By this he meant organization, control, assignment of appropriate ranks to officers, regulation of supply routes, and the provision of principle items used by the army. [62] These matters certainly have bearing in cyberspace, but the term as defined by Sun Tzu is much too broad and general in nature to attempt to draw relationships to cyber power.

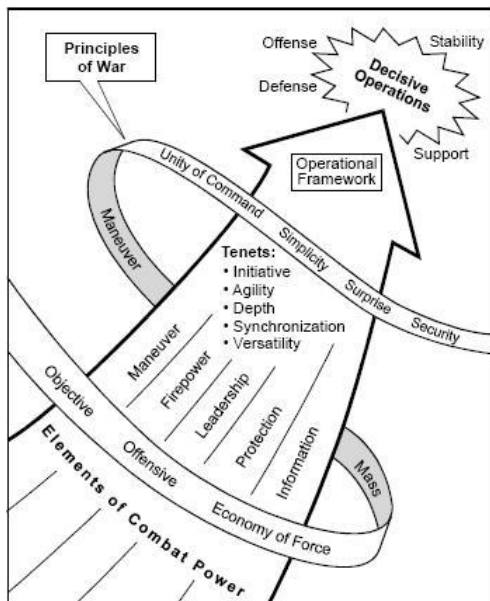
If Sun Tzu is the embodiment of the Eastern military philosophy of unlimited warfare and winning without fighting, then Carl von Clausewitz is the embodiment of Western military philosophy and usage of force against a certain defined selection of targets. Carl von Clausewitz was a Prussian soldier and strategic thinker who lived during the 18<sup>th</sup> and 19<sup>th</sup> centuries and who further defined and refined Sun Tzu's work with experiences of his own some 2,300 years later. That no other definitive work had been written on the subject in 23 centuries attests to the strength of Sun Tzu's ideas, but differing Western viewpoints and advances in technology had finally called for a reworking of his tried and true ideas. Clausewitz spoke much more definitely about the derivation and grand strategy of power on land. He recognized and defined war as "an act of force to compel our enemy to do our will," and "nothing but the continuation of policy with other means," with the aim being the disarmament of the enemy, for "so long as I have not overthrown my opponent, I am bound to fear he may overthrow me. Thus I am not in control: he dictates to me as much as I dictate to him." [12] Besides advocating that the maximum use of force be brought to bear against certain targets which he termed *centers of gravity* (discussed previously), Clausewitz also wrote about five elements of land strategy which were analogous to

Sun Tzu's five fundamental factors. His were moral, physical, mathematical, geographical, and statistical. [12] The first, moral, exactly relates to Sun Tzu's first factor of moral influence. [12] Obviously, the moral imperative is quite a strong influence over relative power if it made it into Clausewitz's list unchanged. Secondly, the physical element "consists of the size of the armed forces, their composition, armament and so forth." [12] This is a new addition, as Sun Tzu took for granted an army strength of "1,000 fast four-horse chariots, 1,000 four-horse wagons covered in leather, and 100,000 mailed troops," [62] while Clausewitz took into account the fact that combat operations in his day could take place between much smaller forces, and that there could be several autonomous armies with different objectives to achieve on different battlefields. [12] Third, the mathematical element "includes the angle of lines of operation, the convergent and divergent movements wherever geometry enters into their calculation." [12] This can be loosely related to Sun Tzu's command factor; while not exactly what he would have meant by the term, it is leadership who formulates and chooses the best mathematical approach for the campaign. Fourth, the geographical element "comprises the influence of terrain, such as commanding positions, mountains, rivers, woods, and roads." [12] This directly relates to Sun Tzu's third factor, terrain. Although we see that technology had advanced far enough to make weather less of a factor in ground warfare, terrain (geography) still made it into Clausewitz's list (at the time of his writings, cavalry had still not been replaced by mechanized units). And lastly, the statistical element which "covers support and maintenance," [12] directly relates to Sun Tzu's "doctrine" factor.

With cyber power, the moral imperative still carries weight. It might be easier to decide about ruining a country's finances because nobody is killed in the attack, but this does not mean that we should. Likewise, the physical element has bearing because, while much smaller in numbers than a traditional army, a "cyber army" must still be comprised of highly skilled and knowledgeable individuals with cutting-edge tools. The mathematical element plays a large role in cyber operations, because knowing what and how you will affect other, related entities based upon your target selection is key to neutralizing centers of gravity without excessive collateral damage. The fourth, geographical, has no bearing upon cyberspace – for reasons mentioned previously – but also largely because IPs are logical and static. Therefore, the router being attacked may as well be in the next room as in China for all the difference it makes (EW being the exception) and the fifth, statistical, has very little bearing; a little office space and a few computers deep within friendly territory is all that is needed (again barring EW) to run a highly

effective cyber force.

The modern United States Army has seen fit to once again reformulate the five elements of land strategy and dubbed them "elements of combat power." These are: maneuver, firepower, leadership, protection, and information. [69] Maneuver directly correlates to Clausewitz's mathematical element, as both concern the geometric movements of units around a battlefield. FM 3-0 defines it as "the employment of forces, through movement combined with fire or fire potential, to achieve a position of advantage with respect to the



**Figure 3 - Fundamentals of Full Spectrum Operations. [33]**

enemy to accomplish the mission.” [69] In network operations however, there are no positions of advantage. Operations occur from fixed IPs and travel along a series of known routes to their ultimate destination (note again that positions of advantage may manifest in Electronic Warfare (EW) however, as this field is more akin to “traditional” kinetic warfare). The second element, firepower, relates to the physical element. [69] The change in word choice definitely reflects the modern assumption that greater numbers do not necessarily compensate for greater technology. Indeed, the U.S. is outnumbered in most of the wars it engages in. The disparity is made up by technologies, which are dubbed “force multipliers.” The Army defines firepower as “the amount of fires that a position, unit, or weapons system can deliver,” with fires being “the effects of lethal and nonlethal weapons.” [69] Firepower is also important to cyber operations, and can be viewed as the potential amount of destruction that a cyber attack (computer network attack or electronic warfare) can cause. Note that this does NOT refer to numbers. A botnet of 100,000 machines used for a DOS attack would have a very low firepower since they are just sending network requests (e.g., to a web server), rather than using malicious or destructive logic. However, the botnet WOULD be using the principle of mass to achieve greater effect. FM 3-0 also goes on to say that “firepower magnifies the effects of maneuver by destroying enemy forces and restricting his ability to counter friendly actions; maneuver creates the conditions for the effective use of firepower.” [69] This statement is not true in cyberspace, for in the machine environment conditions are always ripe to make effective use of firepower. If you have the enemy IP, you may “fire” at it at will. The next element of combat power is leadership:

*Because it deals directly with soldiers, leadership is the most dynamic element of combat power. Confident, audacious, and competent leadership focuses the other elements of combat power and serves as the catalyst that creates conditions for success. Leaders who embody the warrior ethos inspire soldiers to succeed. They provide purpose, direction, and motivation in all operations. Leadership is key, and the actions of leaders often make the difference between success and failure, particularly in small units. [69]*

While this is definitely true for any team to be successful, certain aspects of traditional leadership do perhaps take on a role of somewhat lesser importance or are deemphasized in a cyber force. Without the threat of imminent bodily harm, a dashing and courageous leader is not required to inspire the men to plunge once more into the breach, go over the top, or take the hill. A cyber leader should be analytical, intelligent, logical, decisive, and able to visualize complex interrelationships.

The geographical strategic element has been dropped from the list because technology has mostly (but not altogether) overcome the disadvantages inherent in or afforded by one terrain over another. Mechanized infantry, armor, and artillery divisions have replaced foot-soldiers, horse cavalry, and cannon. The omission of geography works just as well for cyberspace, as we have discussed the uniformity of terrain previously. Surprisingly, the statistical element has also been dropped from the elements of combat power. This is puzzling, as supply lines have always played a huge role in sustaining combat power on land since the dawn of time and continue to do so. Perhaps because of our increasingly globalized environment, the Army may be taking too much for granted about the superiority of modern logistics to supply their war machine across the world. The statistical element can, however, be successfully removed from cyber power as all that is required is a relatively small office space and a few computers far behind friendly lines. In place of these two deletions, the Army added two new ones. The first is a protection element, which is defined as “preservation of the fighting potential of a force so the commander can apply maximum force at the decisive time and place... Protection has four components: force protection, field discipline, safety, and fratricide avoidance.” [69] All four of these components have corollaries within cyber operations to either a greater or lesser extent, with the first being by far the most important. Although cyber warfare favors the offense, defense from



attack and protection of your infrastructure is also of extreme importance as certain portions of the cyber environmental landscape are also the CoGs the enemy is attacking. The other three components, while important, carry lesser weight in cyber operations; there are few kinetic weapons to accidentally discharge, the work mainly takes place in an office environment, and operators are unlikely to accidentally hack a friendly server or launch a malicious logic attack on a friendly IP (although destroying an enemy asset that another friendly entity wished to remain operational is still a concern). The second new element is information, which is described as something that “enhances leadership and magnifies the effects of maneuver, firepower, and protection.” [69] The text goes on to describe the information element in greater detail:

*The common operational picture (COP) based on enhanced intelligence, surveillance, and reconnaissance (ISR) and disseminated by modern information systems provides commanders throughout the force with an accurate, near real-time perspective and knowledge of the situation. Information from the COP, transformed into situational understanding, allows commanders to combine the elements of combat power in new ways. For example, superior understanding of the situation allows commanders to avoid enemy engagement areas, while concentrating fires and maneuver at the decisive place and time. [69]*

The informational element is likewise extremely important to cyber operations, and for the same reasons. Superior knowledge of enemy cyber infrastructure, capability, and defenses are invaluable to planning effective attacks at the proper place and time. Furthermore, it is cyberspace itself that enables ISR and a COP to be developed in the first place.

As we have seen, power on land is primarily about bending an opponent to your will. Sun Tzu advocated winning wars without fighting. Clausewitz said that warfare was essentially a political act and that wars would be one by focusing on the enemy’s centers of gravity with all possible force. While Sun Tzu exercised any means necessary to secure victory (i.e., unrestricted warfare), Clausewitz wrote that diplomacy and spying were better left to political leaders, not military ones. [12] Even though the teachings of Sun Tzu and Clausewitz may differ, lessons can

still be learned and applied from both of them. East versus West viewpoints towards warfare still exist to this day, with China generally following Sun Tzu [31, 81] (and doing quite well at engaging the United States economically) [39], while the United States follows Clausewitz and seeks to win wars by destroying a nation's will to fight. Power at sea, on the other hand, is quite different.

### **Power at Sea**

*The profound influence of sea commerce upon the wealth and strength of countries was clearly seen long before the principles which governed its growth and prosperity were detected... wars arising from other causes have been greatly modified in their conduct and issue by the control of the sea.*

- Alfred Thayer Mahan

The above quote is startling in its obvious similarities to cyberspace. In fact, if cyber warfare bears the least resemblance to land warfare, it appears to most resemble warfare at sea. In Mahan's quote above, changing "sea commerce" to "e-commerce" and replacing the words "the sea" with "cyberspace", one sees natural parallels between the maritime domain and cyberspace. Mahan was perhaps the greatest thinker in naval strategy and doctrine. One might say that Mahan is to sea power as Clausewitz is to land warfare. Mahan's influence on the development and application of US naval power are quite evident, and naval doctrine did not really change much until 1992 with the publication *From the Sea*, which marked a shift in thought from blue water operations to power projection and control of the littoral regions.

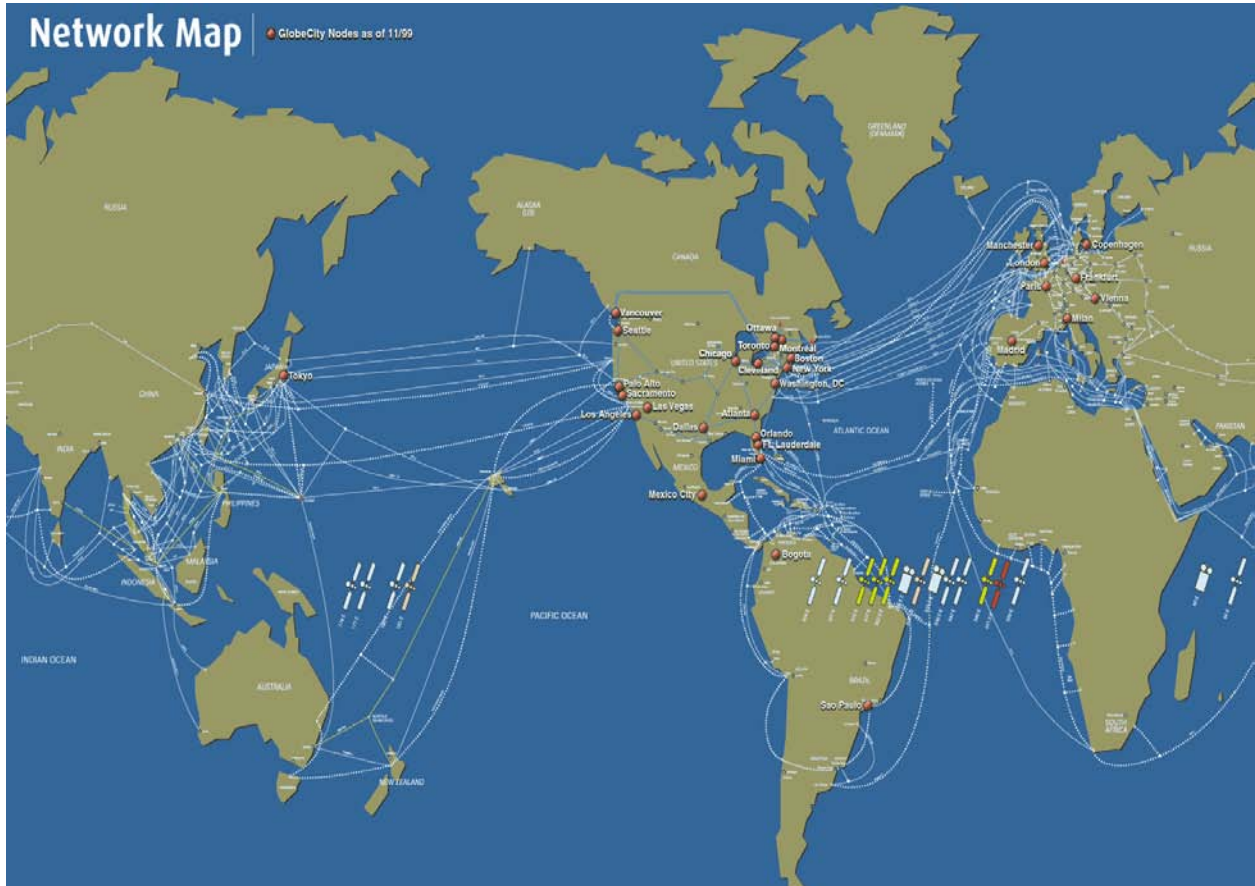
Mahan characterized the maritime domain thusly:

*The first and most obvious light in which the sea presents itself from the political and social point of view is that of a great highway; or better, perhaps, of a wide common, over which men may pass in all directions, but on which some well-worn paths show that controlling reasons have led them to choose certain lines of travel rather than others. These lines of travel are called trade routes; and the reasons which have determined them are to be sought in the history of the world. [42]*

Again, it is easy to see the parallels with cyberspace. Cyberspace is all about connectivity. The internet refers to the globally interconnected network of smaller networks. It includes everyday users at the individual level, business networks, college campuses, and government enclaves. These networks are linked through physical and logical connections. Users connect to cyberspace using fixed (i.e., wired and fiber optic gateways) or mobile (wireless) access points and and “navigate” through cyberspace using the World Wide Web and other virtual protocols. Cyberspace is structured in that there are technical, international, and legal standards for activity, but it also has an unstructured “high seas” nature of how people use the domain. The relative anonymity of the internet allows for malicious behavior without fear of being caught, prosecuted, or otherwise countered. The use of the term “pirate” to describe those who people who use the internet for illegitimate purposes certainly reinforces the parallelism between the two domains. It is difficult—even with advanced technology—to counter a small gang of sea pirates who use guerrilla tactics, much in the same way it is difficult to track down hacker groups and people who are illegally distributing intellectual property.

Another interesting parallel between the two domains is that both have lines of communication (LOCs). Navies were established primarily to combat piracy and protect commerce. Mahan believed that a fleet of warships was required to establish control of the sea by destroying an adversary’s capital ships and then enforcing a blockade to starve him to capitulation. The blockade could be implemented by closing the enemy’s ports and interdicting the flow of commerce and goods on the high seas. Because of the geographic scope involved, it is easier to instead control the choke points through which the LOCs flow; for example, to restrict traffic flow into and out of the Mediterranean, one could simply seize and control the Strait of Gibraltar, the Suez Canal, and the Bosphorus strait. Cyberspace offers similar lines of

communication, as shown in Figures 22-24. As we can see, these network maps look strikingly like shipping lanes. Disrupting the flow of information in cyberspace (i.e., a digital blockade) could be achieved through direct action against the nodes (ports) or the LOCs (communications



**Figure 4 - The Well-Worn Paths of Cyberspace – Undersea Cables. [88]**

links) using kinetic strikes, computer network attack, and electronic warfare, or some combination of the three. Navy doctrine stresses the importance of these lanes and ports and the danger of allowing uncontested access to them as follows:

*Because we are a maritime nation, our security strategy is necessarily a transoceanic one. Our vital interests—those interests for which the United States is willing to fight—are at the endpoint of “highways of the seas” or lines of strategic approach that stretch from the United States to the farthest point on the globe. [14]*

This holds just as true in cyberspace, and perhaps even more so. At the end of shipping lanes are ports, but destruction of these ports does not affect the sea domain itself, just the ability to exploit the sea using that port. In cyberspace, the devices that make up the “ports” also make cyberspace what it is. Shutting off a network router or web server in essence degrades (if not destroys) that particular portion of cyberspace. Centers of Gravity may be connected directly to these paths, and their destruction could result in actual removal of areas of the domain, and

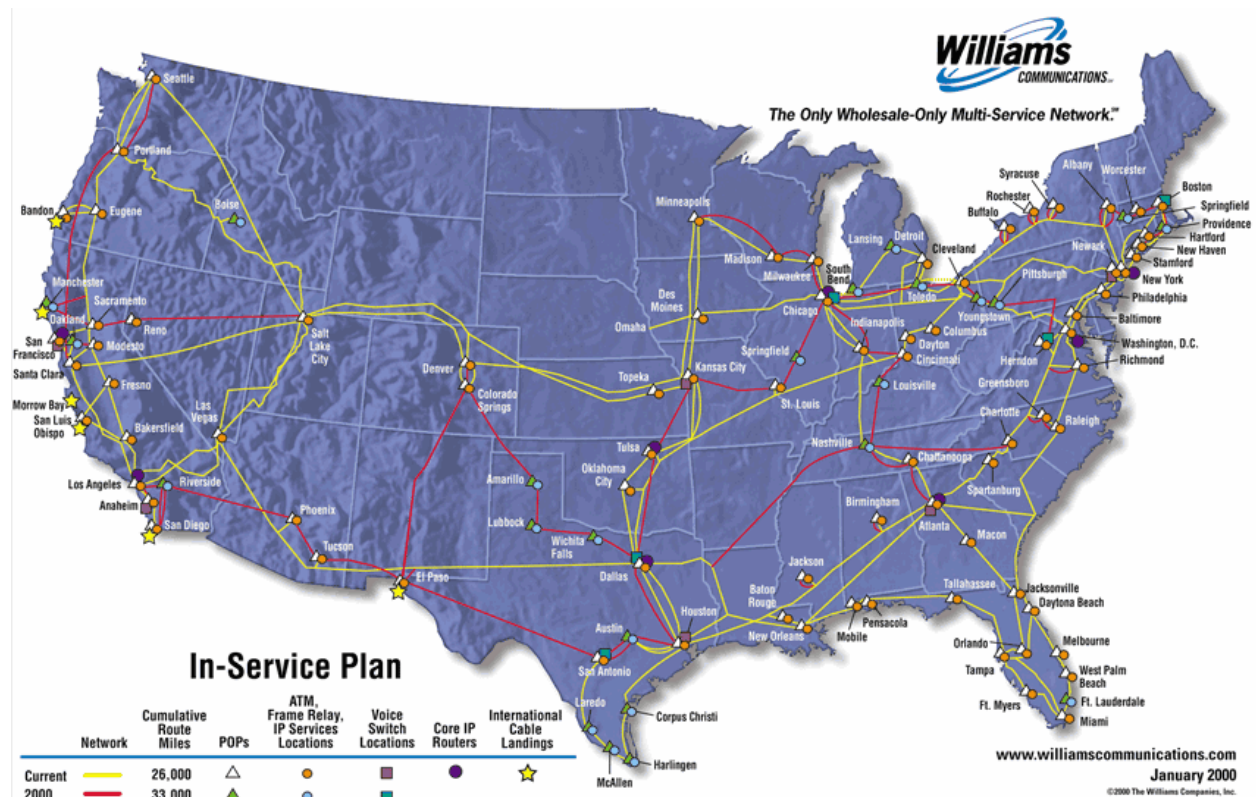


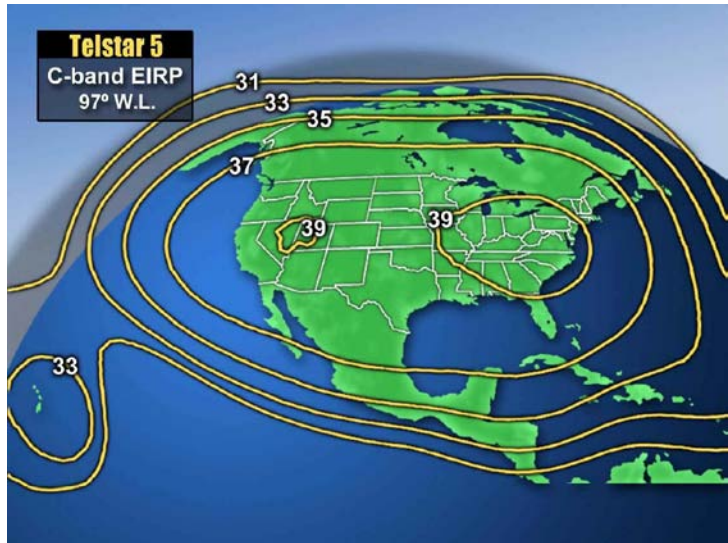
Figure 5 - The Well-Worn Paths of Cyberspace - Internet Backbones (not all-inclusive). [89]

significant harm to the nation. In other words, destroying a country’s ports—whether sea ports or cyberspace nodes—is a means to an end (e.g., surrender or remain neutral). A difference between the two domains is that actions in cyberspace may very well change the “terrain” of cyberspace. Regarding planning and conduct of naval operations, Mahan wrote the following (with comments inserted to highlight application to cyberspace):

*Before hostile armies or fleets [cyber forces] are brought into contact (a word which perhaps better than any other indicates the dividing line between tactics and strategy), there are a number of questions to be decided, covering the whole plan of operations throughout the theater of war. Among these are the proper function of the navy [cyber forces] in the war; its true objective; the point or points upon which it should be concentrated; the establishment of depots of coal and supplies [cyberspace infrastructure]; the maintenance of communications between these depots and the home base [sustain cyberspace domain]; the military value of commerce-destroying as a decisive or a secondary operation of war; the system upon which commerce-destroying can be most efficiently conducted, whether by scattered cruisers [cyber attack capabilities] or by holding in force some vital centre through which commercial shipping [information] must pass. [42]*

And so we have the same question faced by the Navy: should a cyber force restrict itself to attacking only military targets? Or should it apply itself to the destruction of a nation's commerce; a so-called "guerre de course?" The question has been answered previously in this

paper, and remains that the only CoGs reachable in cyberspace are financial, economic, and informational. It is not possible to cause capitulation by attacking military assets in cyberspace, and therefore should only be done in support of another branch of service's mission or to defend your own country's territory or assets.



**Figure 6 - The Well Worn Paths of Cyberspace - Critical Satellite. [90]**

Until the 1920's, the great oceans separating the United States from other nations were considered a buffer against attack; a part of our natural defenses which any enemy must cross in order to do us harm. When aircraft could fly over the oceans, the Air Force also became part of that defense. Now that both the air and sea may be bypassed—quite quickly, no less—the first line of defense for any technologically advanced nation will reside in cyberspace. Dr. Lani Kass,

former Director of the Air Force's Cyberspace Task Force and Special Assistant to the Chief of Staff of the Air Force agrees, stating: "The first battle in the wars of the future will be over the control of cyberspace." [10] However, Mahan recognized that:

*The control of the sea, however real, does not imply that an enemy's single ship or small squadrons cannot steal out of port, cannot cross more or less frequented tracts of ocean, make harassing descents upon unprotected points of a long coastline, enter blockaded harbors. On the contrary, history has shown that such evasions are always possible, to some extent, to the weaker party, however great the inequality of naval strength. [42]*

This assertion is borne out by modern Navy doctrine as well:

*"Control of the sea, however, has both spatial and temporal limits. It does not imply absolute control over all the seas at all times. Rather, control of the sea is required in specific regions for particular periods of time, to allow unencumbered maritime operations." [16]*

This is surely true for cyberspace as well. The only difference is that while small forces slipping out of a naval blockade may cause little harm, small commands or file uploads slipping past a cyber blockade could unleash a self-replicating virus that infects and crashes countless servers and desktops. Therefore, passive containment and defense is not what is called for. In order to stop the cyber enemy from slipping past your blockade to attack your digital shores, you must destroy him, just as the Navy and the other branches of service advocate within their respective domains. As Mahan said:

*There is defence pure and simple, which strengthens itself and awaits attack. This may be called passive defence. On the other hand, there is a view of defence which asserts that safety for one's self, the real object of defensive preparation, is best secured by attacking the enemy. [42]*

Likewise, modern navel doctrine states: "War at sea emphasizes the offensive, bringing to bear information, intelligence, and tactical initiative against an adversary." [16] Similarly, passive defense does not lend itself well to Cyberspace. The longer you lie still and allow an enemy to beat on your doors, the longer you give them to find a way around or through you.

Mahan postulated that there are six conditions affecting the sea power of nations. These are geographical position, physical conformation, extent of territory, number of population, character of the people, and character of the government. [42] Most of these conditions do not hold for cyber power, as we shall see.

First, geographical position was important to Mahan in that if a “nation were so situated that it is neither forced to defend itself or induced to seek extension of its territory by way of land, it has, by the very unity of its aim directed upon the sea, an advantage as compared with a people whose boundaries are continental.” [42] In Cyberspace, geographical position is unimportant except for a kinetic attack. Anyone may attack anywhere at any time as long as the host is connected to the internet. Servers may be hosted in other countries, and infrastructure may be owned by another nation’s corporations, but location in cyberspace is logical (virtual) and as of yet host internet protocol (IP) addresses do not change easily.

Secondly, when Mahan spoke of physical conformation, he was referring to the seaboard of a nation and whether it was long or short and whether it had many deep harbors or not. [42] Physical conformation can be said to play a role in cyber power. If a nation is connected by “fat pipes” such as OC-768 they will have a bandwidth advantage over nations with smaller ones. This will help with the launching or absorbing of botnet DOS attacks and the effects of wildly propagating virus traffic, but has little effect on more elegant single-target intrusions or attacks. Furthermore, since cyberspace is a man-made environment, humans can shape its conformation to their will. The placement of firewalls, routers, etcetera all have an effect on security and therefore afford more relative power.

Third, by extent of territory Mahan had reasoned that the more coast-line a nation had (assuming the sufficient amount of manpower to garrison it), the more sea power it could bring



to bear. [42] This element does not play a role in cyber power. In fact, having a large presence in cyberspace places you at more risk since you have more area to defend. Having more real estate in cyberspace means you must also spend more to safeguard what you have, but does not mean you also gain more offensive capability, offense being related to intelligence and not mass. The one caveat to this is again botnets for DOS attacks, but such attacks are extremely crude and do not cause lasting damage.

Fourth, number of population, is somewhat important but not for the same reason it is in determining sea power. For Mahan, it was important because bodies “readily available for employment on ship-board and for the creation of naval material” [42] were something easily procurable, as the profession could be taught to most anyone. As it relates to cyber power, which needs relatively few but yet highly skilled people, number of population matters only in that it increases the pool and chances that you will have some of these individuals available to utilize in the defense of the nation.

The fifth element, national character, was important to Mahan in that he believed the character and aptitudes of the people would affect the development of sea power. “If sea power be really based upon a peaceful and extensive commerce, aptitude for commercial pursuits must be a distinguishing feature of the nations that have at one time or another been great upon the sea.” [42] This element holds for cyberspace. The internet is mainly a tool for commerce and flow of information and knowledge. Commercial interests will always research and develop cyberspace technology if it affords them more capital, and users will always innovate if it affords them more utility and knowledge. Any nation which rises to greatness in cyberspace will have a love of commerce and knowledge.

Lastly, the character of the government was put forth by Mahan as the sixth element determining the sea power potential of a nation. He noted that “a government in full accord with the natural bias of its people would most successfully advance its growth in every respect,” [42] and indeed this seems to be the case in regards to cyberspace as well. The United States—capitalistic as it is—surely loves commerce as much as its people do, and as a result is the largest innovator of cyberspace technology in the world: The internet originated in the United States, it hosts 6 of the 13 world-wide root domain servers, and American-designed router, switch, firewall, and intrusion detection systems are produced in and sold to countries world-wide. Its love of the freedom of knowledge has been called into question as of late, but so far no great strides have been taken to stem its flow. Should a government fall out of accord with its people, its power in cyberspace would surely suffer, as vulnerabilities would no longer be called to authorities’ attention but kept safe for private use.

These elements of sea power have stood the test of time, and nations’ power at sea have peaked and ebbed according to their dictates throughout the pass of centuries. Today, the sea and cyberspace both play more of a role than ever in the commerce of a country:

*World economic stability depends upon vigorous transoceanic trade. Today, 90% of the world’s trade and 99% of our import-export tonnage is transported on the sea... Ensuring that the world’s sea lanes remain open is not only vital to our own economic survival, it is a global necessity. [16]*

Along the same lines, e-commerce sales in 2008 reached a value of \$204 billion. [56] Obviously, both the sea and cyberspace are extremely important economic landscapes. Mahan believed that naval strategy should not only promote sea power during times of war, but also during peacetime in order to protect this wealth of nations. “Naval strategy has indeed for its end to found, support, and increase, as well in peace as in war, the sea power of a country.” [42] This statement

obviously holds true for cyberspace as well. Let's take a look at how the modern US naval strategy aims to gain sea power and then relate their policies to cyber power.

The modern Navy emphasizes control of the sea as the greatest goal during warfare. And indeed, the ability to control, whether it be the sea, of air, or cyberspace is always a measure of the power you possess. Naval Doctrine Publication 1, Naval Warfare states that control of the sea can be accomplished through decisive operations by:

*Destroying or neutralizing enemy ships, submarines, aircraft, or mines. Disabling or disrupting enemy command and control. Destroying or neutralizing the land-based infrastructure that supports enemy sea control forces. Seizing islands, choke points, peninsulas and coastal bases along the littorals. Conducting barrier operations in choke points that prevent enemy mobility under, on, or above the sea. [16]*

Looking for similarities, we find many that we can apply to the control of cyberspace. The first, destroying or neutralizing the machines of war, is difficult in cyberspace. Unlike building a strong navy—which requires a tremendous investment and industrial capacity—building a cyberspace capability is relatively cheap. The computer on which an enemy hacker plies his trade is of the utmost unimportance and easily replaceable. It is the hacker himself, his knowledge and intelligence that is the true weapon. Therefore, the first item on the Navy's list might say "Locate and destroy or neutralize enemy cyber combatants," if we are to apply it to cyberspace. Next, disabling or disrupting enemy command and control is highly important, regardless of the warfighting domain and is critical in controlling that domain. Third, destroying or neutralizing the enemy hacker's control infrastructure (how the enemy communicates targets and priorities to combat assets) may not map to cyber power, as distance from command and control is not a prerequisite to controlling a cyber force as it is in a naval force. Combat forces may even be co-located with leadership, and therefore controlling a hacker may be as easy as shouting down the hall at him. Destruction of the actual physical infrastructure of cyberspace,

however, is a highly effective means to countering an enemy's ability to attack, albeit counterproductive to forces wishing to capture and control it. Fourth, seizing islands, choke points, peninsulas and coastal bases could be compared to seizing control of key routers and entry points that connect an entity to the outside world, and lastly, conducting barrier operations in choke points to prevent enemy mobility is a task that can also be accomplished in cyberspace. Once you hold the key routers as partially illustrated in the above figures of the "well-known routes of cyberspace," a country could be isolated very rapidly from the rest of the world.

But what exactly does all this control gain us? The Navy recognizes that the control of the sea allows them to:

*Protect sea lines of communication, deny the enemy commercial and military use of the sea, establish an area of operations for power projection ashore and support of amphibious operations, and protect naval logistic support to forward deployed battle forces. [16]*

The first two are very important results of the control of cyberspace as well, and the last two are not. Communication of commands, communication of information, and communication of commercial transactions are the whole purpose of cyberspace, and so protecting them are obviously of the utmost importance. Denying the enemy commercial and military use of cyberspace is equally important, considering much of the warfighting capabilities of the other branches of service rely on cyberspace to operate. Also, the asymmetric nature of cyberspace means that technologically advanced nations will usually have more to lose in cyberspace than less advanced nations. Establishing an area of operations for power projection could be a factor for cyber power. This includes the home-based infrastructure as well as gaining access points into adversary networks. Lastly, projecting logistic support to forward deployed battle forces does not play a significant role in cyber power. However, providing tactical support may if

special cyber capabilities are to be embedded within Special Forces or regular army units as they move forward across a hostile territory or battlefield.

Now that we know why power at sea is important, what elements influence its potential, what power at sea means, and what it affords you, let us talk briefly of the two styles of warfare the Navy recognizes and see if we can apply them to cyberspace.

*The United States Navy recognizes and practices two styles of warfare. These two styles are termed Attrition Warfare and Maneuver Warfare. In the first, naval forces set out to destroy as many of the enemy naval assets as possible over a period of time, essentially wearing down the enemy. In the latter ...it emphasizes the need to give the commander freedom to deal with specific situations. Maneuver warfare is further characterized by adaptability and is not limited to a particular environment. [16]*

Both of these styles are applicable in cyberspace as well. Attrition warfare only works when one side can develop, sustain, and generate replacements for forces and equipment that have been lost. Eventually one side is driven to the point at which it can no longer generate combat power, or decides that the cost of continuing the conflict has become prohibitive. As discussed earlier, information technology devices are relatively cheap, so attrition of combat capability would seem more applicable to the destruction of talent. It takes time to identify, educate and develop cyber warriors with the appropriate skill sets, which is similar to the length of time required to manufacture capital ships. A similar situation occurred in WWII when the German Luftwaffe suffered severe attrition of its pilots. Late in the war, most of Germany's experienced pilots had been capture or killed, and the ones coming out of flying school were no match for Allied pilots. Maneuver warfare is perhaps more important and relevant. Cyber warfare is the ultimate in maneuver warfare—cyberspace compresses time and space (much like aircraft did compared to ground vehicles). A cyber attack can occur at any time, at any place, with little or no warning. In the physical domains, it is possible to detect an adversary preparing for military action—movement of troops, ships and aircraft—but there is no real early warning system for cyber

attack. Response time is also a significant challenge in that by the time a cyber attack has been detected and attributed (which in and of itself may be very difficult), it may be too late to respond in a meaningful manner. Cyber defenses and systems will need to become more autonomic, free to make rapid decisions regarding the safety of their assigned areas of operation. Again, this is similar to the Navy's distributed command and control philosophy, known as command-by-negation, in which ship commanders are afforded a great amount of autonomy and discretion in the conduct of their missions. This is necessary for the Navy because its commanders operate far away from their higher headquarters. Having to call back for guidance and decisions was not feasible due to the time constraints. This is an interesting paradox with cyberspace. On one hand, because it compresses time and space, the information *can* be transmitted to and from headquarters quickly. However, the speed and lack of warning of attacks in cyberspace tend to question whether a centralized command and control structure would really work for cyberspace defense.

As we have seen so far, cyber warfare shares the least in common with warfare in the Land domain, since terrain, maneuver (not to be confused with the "maneuver" principle of war), and fires play less of a role in cyberspace. We have also seen that war in the cyber domain shares many parallels with the sea, in that both are domains characterized by economic and informational trade which flows along certain paths that may be blockaded, and that commanders must have the autonomy to make quick but far-reaching decisions. Now let us turn to the domains of Air and Space to see what lessons we may apply to cyberspace.

### **Power in the Air and Space**

*The European War was only the kindergarten of aviation. It had machines that were just invented, the possibilities of their use were just beginning to be understood by the aviators themselves, while others looked on them as strange creations that were defying all known laws of science, of custom and of war.[35]*

*-William "Billy" Mitchell*

Like sea, the air domain has many parallels with cyberspace. The similarities include the fact that cyberspace enables and affects the other domains; the fact that cyberspace compresses time and space, allowing forces to “fly over the terrain” and strike at the enemy’s interior; and the importance of controlling the cyberspace domain to facilitate control in the other domains.

As with the other domains, certain names stand out regarding airpower theory. They are Giulio Douhet and Billy Mitchell. Their histories were discussed previously; we will now delve directly into their theories, doctrine, and strategy.

Douhet was a proponent of a strategic, offensive air force while Mitchell advocated a more tactical, offense/defense balanced force. Douhet wrote: “[The Air Force] is an offensive force which can strike with terrific speed against enemy targets on land or sea in any direction, and can force its way through any aerial opposition from the enemy.” [23] This flavor of air power lends itself well to an absolute war carried out through cyberspace. It is true that cyber warfare favors the offense, and like an air force, a cyber force may strike at lightning speed on a global level. It can force itself through any opposition as well (since the enemy cannot completely disconnect itself and still retain functionality), but not with mass as Douhet suggested nor stealth as modern Air power prefers. Intelligence and cunning logic are the weapons that will eventually defeat any cyber defense. Douhet was a follower of the Clausewitzian school of thought and believed that the goal of air power was to “inflict the greatest damage in the shortest possible time.” [23] He would have loved absolute cyber war, where massive damage can be caused in the blink of an eye. Additionally, Douhet wrote “Like a cavalry corps, whose best defense is always to attack, the air arm depends upon attack for its own best defense, to an even greater degree, in fact.” [23] This can also be said of cyber power, which so greatly favors the offense. Douhet also believed that the control of the air should be used to destroy “the vital

centers” of the enemy, or his will to fight and industrial backbone, and that it should be done with the maximum amount of force possible. [34] This, particularly, is pure Clausewitz and works very well in an absolute cyber war. However, he also wrote: “We must resign ourselves to the offensives the enemy inflicts upon us, while striving to put all our resources to work to inflict even heavier ones upon him.” [23] This, of course, is not true in cyberspace. Defenders in cyberspace need not resign themselves to enemy offenses, as there are many methods and means of defense which may be effective in blocking damage to the possible centers of gravity residing there. Because of this, even though cyber power favors the offense, defense cannot be neglected.

Mitchell’s ideas, on the other hand, take aerial defense into much more consideration and lend themselves well to a limited cyber war where the force is providing support to operations in other domains. Even though he was of the strong belief, as was Douhet, that air power was supremely important and a force which would determine the victors of future wars, he still wrote “Of course, everything begins and ends on the ground. A person cannot permanently live out in the sea nor can a person live up in the air, so that any decision in war is based on what takes place ultimately on the ground.” [47] Mitchell also said “you will never eliminate the land forces entirely from the air, but you will greatly affect them.” [35] He saw air power as a more tactical force than did Douhet. He explains: “[Attack aviation’s] specific mission is to attack troops, trains of automobiles, convoys, railroad trains, tanks, debarkations from trains, ships or vessels, warships, or any military object on the ground or the water which exposes itself to attack from the air by cannon, machine guns, or lightweight bombs.” [45] Mitchell’s ideas are currently being applied in certain limited cyber engagements. Whether it is being put to use disabling or confusing early warning radars or IADS for air forces or denying or disrupting adversary



communications for land forces, cyber power is already being used in these limited, tactical fashions. One has but to look to Russia's invasion of South Ossetia to find an example.

Mitchell and Douhet agreed that the Air would become a decisive field of battle and that the control of the air would dictate a win or a loss for the entire war. Douhet wrote that the goal of Air power was "to conquer command of the air—that is, to put the enemy in a position where he is unable to fly, while preserving for one's self the ability to do so." [23] while Mitchell wrote "Should a nation, therefore attain complete control of the air, it could more easily master the earth than has ever been the case in the past" [47] This is also extremely valid in the case of cyberspace, but only against nations who are reliant upon it. If a nation is used to waging war in a "primitive" non-net-centric fashion, the denial of cyberspace will have little effect on the overall outcome. This is true of asymmetric conflict in which the two combatants will select the style of warfare (e.g., guerilla or attrition) that best fits their situation and constraints. However, if the nation being attacked has also become reliant upon net-centric warfare as we have, then the denial of cyberspace will greatly diminish the power of their military forces; this is especially true if people have forgotten how to function without cyberspace.

Modern air power doctrine sides more with Mitchell's theories than with Douhet's, not because Douhet's ideas have been disproven, but because American 21<sup>st</sup> century values, ideals, and morals preclude the use of overwhelming destructive power upon a nation's cities and populace. However, the strategic nuclear option has not been taken off the table for use in cases of extreme necessity. Our air force is much more tactical than it was in WWII, Korea, Vietnam, and the Cold War because of the technological leaps that were made in the late 80's and early 90's with "smart" weaponry and guided munitions. Strikes from the air have become extremely surgical. Carpet bombing cities is no longer necessary to achieve an objective; targets of value

may be singled out and destroyed with very little collateral damage. Technology has also changed the meaning of Mass. Whereas Mass used to mean hundreds of airplanes in the air, flying a formation into enemy territory, it can now be achieved with just one B-2 bomber and its massive 40,000 pound payload of independently targeted munitions. [58] This is similar to cyber power in that mass can be had with just one computer and the right exploit, payload, or malicious logic.

The US Air Force also embraces the nine Principles of War (including Mass as we have discussed it in the previous paragraph). In addition to those, they have added seven Tenets of Air and Space Power. They are: Centralized Control and Decentralized Execution, Flexibility and Versatility, Synergistic Effects, Persistence, Concentration, Priority, and Balance. [63]

*Centralized control* is defined as “the planning, direction, prioritization, synchronization, integration, and deconfliction of air and space capabilities to achieve the objectives of the joint force commander,” and *decentralized execution* is “the delegation of execution authority to responsible and capable lower level commanders to achieve effective span of control and to foster disciplined initiative, situational responsiveness, and tactical flexibility.” [63] While this tenet may work for the Air Force, who has a limited amount of specific types of aircraft with which to accomplish set goals and objectives, it cannot work for a cyber force for reasons we have discussed earlier such as the need for lightning fast reactions to neutralize incoming threats or to exploit time-critical vulnerabilities such as a new, unpatched system being brought online. Much like the Navy, decentralized control as well as execution is required. Additionally, a Cyber Force would not be constrained by a limited amount of extremely high-dollar, specific use assets.

*Flexibility* “allows air and space forces to exploit mass and maneuver simultaneously,” while *versatility* “is the ability to employ air and space power effectively at the strategic, operational, and tactical levels of warfare.” [63] Both of these are also important to cyber power. Like the air force, a cyber force would also be able to quickly shift from one campaign objective to another, quickly and decisively. Once an integrated air defense radar station is taken down, the soldier/hacker may then focus attention to a new priority such as a communications substation or the power grid. New objectives may be given and attacked on the fly. Likewise, the switch may be made from a tactical objective to an operational or strategic one in an instant. There is no maneuvering of forces or tools, just a new IP and different system architecture.

Continuing, *synergistic effects* mean that “the proper application of a coordinated force can produce effects that exceed the contributions of forces employed individually... the objective [of modern war] is the precise, coordinated application of the various elements of air, space, and surface power to bring disproportionate pressure on enemy leaders to comply with our national will.” [63] While a cyber force may also produce synergistic effects in that it, in concert with forces in other domains, can cause a disproportionate pressure on enemy leaders to comply with our national will, it does not do this quite as well as an Air Force can. The reason is one of observability. While an air force may fly over a battlefield and see firsthand the effects that it is causing and then change its focus to meet new conditions, a cyber force is mostly blind to these subtleties—predicting and measuring cyber effects remains a significant challenge. In the absence of timely, accurate intelligence, the cyber force must infer much as to the enemy’s reactions to its cyber attacks.

Additionally, air and space power is said to offer a unique form of *persistence*: “Air and space power’s exceptional speed and range allow its forces to visit and revisit wide ranges of

targets nearly at will. Air and space power does not have to occupy terrain or remain constantly in proximity to areas of operation to bring force upon targets.” [63] If exceptional speed and range along with unfettered access to attack targets at will is the hallmark of persistence, then cyber power, which travels at extremely high speeds and with unlimited range surpasses airpower in this regard.

*Concentration* means to “concentrate overwhelming power at the decisive time and place,” [63] and is a tenet that also has meaning for cyber power. The Air Force is concerned, and rightly so, with the dilution of power as more and more individuals call on the unique and versatile support that air power brings to the table. This is mainly a function of the limited resources available to the combatant commanders. A cyber force could have much more capability to meet the varying requests for fire support. However, concentration is still important in that hackers should concentrate their mental abilities against the “tough nuts to crack” until their objectives are achieved. In the realm of network and computer exploitation, the more sets of eyes on a problem the better. Someone may catch something that another has missed, or have an idea that hasn’t been tried, thereby making the exploitation quicker. Concentration, however, should *only* be utilized on these difficult targets as it would be a waste to allocate too many talented individuals on simple problems—i.e., economy of force.

*Priority* refers to the need to manage the allocation of scarce assets. Without a centrally controlled prioritization process—that addresses allocation of capabilities and the targets being attacked—air power can be significantly weakened. [63] This is the case with any force, but more so for the Air Force because of the aforementioned lack of resources. Targets must also be prioritized for a cyber force in order of importance, but in some ways, it is much easier to meet the demands likely to be placed upon them in wartime, because cyber attacks do not have the

same logistical issues as conventional air operations (fuel, ordinance, travel times, air frame repair and maintenance, etc.). It is conceivable that a large team of network attackers may engage a target list in very short order from the comfort of their home duty location. EW is a different matter, since EW attack platforms, such as the EC-130, are few in number.

Finally, *balance* refers to the need of an air commander to “balance combat opportunity, necessity, effectiveness, efficiency, and the impact on accomplishing assigned objectives against the associated risk to friendly air and space forces.” [63] A cyber commander must also take these things into account, as they are just as important: opportunity is something that should be pursued, as a vulnerability that exists today may be patched tomorrow; necessity dictates that we accomplish the objectives set forth by the combatant commander and by so doing expedite the war; effectiveness means that we don’t waste time trying to break into systems which would have a low impact on the enemy; efficiency means that we do not wish to spend inordinate amounts of time on well defended systems when there are others that are more poorly defended (the principle of economy of force also applies); and cyber “fratricide,” some examples of which would be the jamming of allied signals, destruction of enemy hosts that some allied unit wanted left intact, or allied soldiers plugging a piece of equipment into an enemy network that has been infected with a coalition virus, should be avoided.

As regards space doctrine specifically, there are no principles, tenets, or ideas not covered by the above general “air and space” doctrine. AFDD 2-2, Space Operations, AFDD 2-2.1, Counterspace Operations, and JP 3-14, Joint Doctrine for Space Operations, all speak in terms of missions, roles, and capabilities, but not of theory. As was mentioned in Chapter II, military space warfare theory is lacking, and this will likely remain so until space becomes a contested environment.

As we have seen, power in cyberspace shares much with power in the air. It is very much a form of maneuver warfare, and is flexible, versatile, and persistent. It affects all of the other domains, is very precise, and concentrates mass into a very small force. It can be used either strategically or tactically, should be employed both offensively and defensively, and should be balanced in its application. Let us now finally turn to cyber power proper.

#### IV. Cyber Power in the 21<sup>st</sup> Century

*Cyber capabilities can assuredly support applications of other force capabilities, but, fundamentally, they are not the destructive, kinetic purveyors of violence that war fighters traditionally envision in planning military strategy, engagements and wars. If we apply them as primary weapons of war, then basic concepts regarding the use of force or threat of force to compel the enemy must change.*

-Sebastian M. Convertino[13]

*...Improvement of weapons is due to the energy of one or two men, while changes in tactics have to overcome the inertia of a conservative class; but it is a great evil.*

-Alfred Thayer Mahan [42]

#### Clarifying the Environment

As we have seen from the examples other domains provide, Mahan was correct when he postulated that environments shape strategy. [42] In order to come to terms, then, with what cyber power is and what it can and cannot be used to accomplish, one must first define cyberspace (the machine environment) and catalogue the warfighting characteristics of its environs. This is a tricky business, as many scholars, politicians, and strategists have already attempted to do just that... but still, 40 years after the “creation” of cyberspace, there is continual argument and redefinition of exactly what cyberspace is. Here are some pertinent DoD definitions:

Cyberspace is “*the notional environment in which digitized information is communicated over computer networks*” [74]

And:

Cyberspace is a “*domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.*” [73]

And:

“*Cyberspace is the nervous system... the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work.*” [28]

And:

*Cyberspace is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” [26]*

The definition that is currently used by the warfighting community is the one put forward by the office of the Deputy Secretary of Defense in its May 2008 memo, subject: The Definition of “Cyberspace” which is quoted directly above. This is a fairly good definition, but it still fails to convey the full scope or reality of cyberspace. First, it is written for an “information environment,” which as was discussed in Chapter II, cannot be an environment. Next, it tries to be all-inclusive by spelling out exactly what comprises Cyberspace, and by so doing has limited its scope to current technologies. Finally, the wording “the interdependent network of IT infrastructures” is most certainly incorrect, as not all networks are interconnected with one another.

A definition that more fully captures the essence of the cyberspace domain’s environment would be as follows: “cyberspace is the logical electromagnetic control network between two or more machines.” This definition is elegant in its simplicity. Omitting terms such as “electronics” does not discount nano- and bio-machines. Replacing “the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” with “network between two or more machines” acknowledges the fact that all systems are made up of individual machines and emphasizes that an un-networked machine cannot really be a part of cyberspace. Further, not all networks have a physical infrastructure (such as mesh networks), and that there are many stand-alone and isolated computer networks. And finally, the wording “logical electromagnetic



control” reduces the complex down to what we are really trying to do - control or affect a machine remotely via electromagnetic impulses or signals. The word “logical” is important, as a high energy burst to disrupt circuits is more of a physical act than a logical one, and therefore does not belong to cyberspace, at least according to this definition. A high energy burst is a tool, much like a bomb is to the land and sea environments. Note that this differs from other opinions which would include directed energy as a form of cyber warfare. [3] The problem with all of these competing definitions is that they depend on the perspective of who is defining the problem and what they care about. For the remainder of this report, the focus will be on the logical/control aspects.

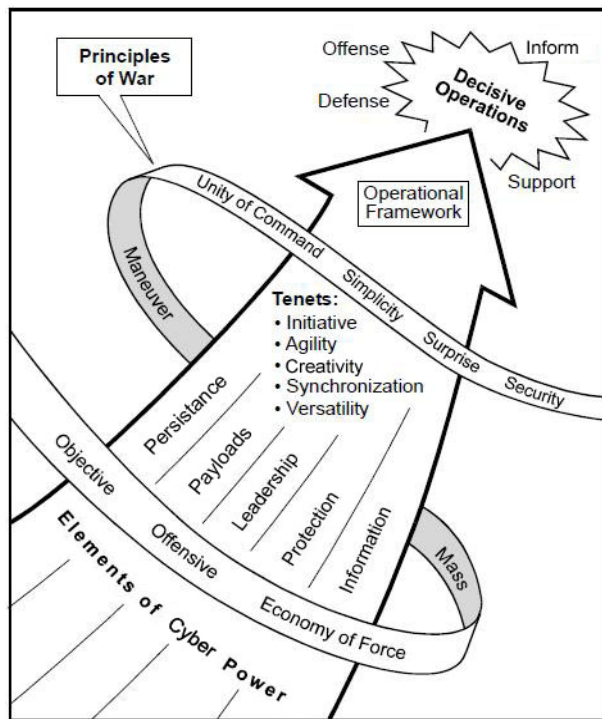
### **Power in Cyberspace**

Extending Billy Mitchell’s beliefs to cyberspace, “Only a cyber force can fight a cyber force. Only a cyber force can keep infrastructure operating, information flowing, satellites in orbit, guided ordinance hitting targets, squads communicating with HQ, and units from getting lost in war.” But what does power in cyberspace mean? There has been no formal definition of cyber power by the DoD; what is meant by the word is taken for granted as being understood. Some attempts by outside scholars have been made to fix the meaning more firmly. Dr. Dan Khuel of the National Defense University defines it thusly: “Cyberpower is the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.” [38] This is a great definition, which illustrates that operations in cyberspace can cause and/or influence events in any or all of the other domains, as well as in its own. Further, he goes on to point out that just like power in any of the other domains, “while cyberspace as an environment simply ‘is’, cyber power is always a measure of the ability to use that environment.” [38] The previous chapter pointed out how each of the current services wield

power (“the ability to do something,” as Billy Mitchell would have said) in their respective domains. Let us explore now how cyber power might “do things” in its domain.

It is very important to recognize the truth of the two quotations quotations (Convertino and Mahan) at the beginning of this chapter when speaking about the development of cyber power. In order to win wars with cyber power, the capabilities of today and into the future must be used in new and innovative ways despite a resistance towards change. Used as it has in the past, cyber power is very effective at playing a supporting role to operations in other domains. In order to come into its own, however, the rules of cyber warfare must be rewritten.

The previous chapter discussed similarities and differences between cyberspace and the



**Figure 7 - Fundamentals of Full Spectrum Cyber Operations**

other domains of warfare. Although the lessons that the domain of land gives to us are few in terms of actual *operations*, they provide much in the way of *ideology* that the Cyber domain would do well to borrow. Shown is the Army’s “Fundamentals of Full Spectrum Operations,” modified for cyber power. Very little needed to be changed from the original figure (Figure 20).

The Principles of War have been carefully cultivated over many years, and as such define such basic truths of warfare in any domain. All of the principles are just as

pertinent to war in cyberspace as in other domains, as discussed previously. The changes occur in the service-specific elements of combat power, their tenets, and types of operations.

## Elements of Cyber Power

Two of the Army's elements of combat power have been changed, while three remain the same but take on different significance. First, persistence has replaced maneuver. Recall the army's definition of maneuver as "movement combined with fire or fire potential to achieve a position of advantage with respect to the enemy." [69] Although there may be certain comparisons to maneuver in cyberspace (such as taking over a system that the enemy network trusts, but is less well protected than the actual target), it is all logical (virtual). In cyberspace, there is no position of advantage (high ground) which affords the attacker an advantage simply by virtue of his holding it. Therefore, persistence is exactly what is required to accomplish the mission. It is possible to win through any cyber defense with persistence. If an attacker tries long enough, hard enough, and creatively enough, he will find and exploit a vulnerability in the target host or application. Persistence is what will eventually give you an advantage over the enemy, and makes it the ideal replacement for maneuver. However if a target is too hardened and time is of the essence, more direct, kinetic approaches may be more appropriate.

Second, firepower has been replaced with payloads. Whereas traditional positions, units, and weapons systems have a limited amount of kinetic firepower that they can deliver, certain cyber assets can deliver an unbounded number of payloads which are only limited by the imagination, knowledge, and talent of the crafter. But regardless of whether your payload is a logical bomb or a kinetic one; a microwave or an electromagnetic pulse; a trojan horse, a worm, or even simple text; "[payloads] magnify the effects of [persistence] by [manifesting the attacker's will] and [disrupting, corrupting, or exploiting enemy systems; persistence] creates the conditions for the effective use of [payloads]." [69] And indeed, what use would persistence be without an effect at the end?

Third, leadership remains the same. Leadership is required to “focus the other elements of combat power and serve as the catalyst that creates conditions for success” and to “provide purpose, direction, and motivation in all operations.” [69] This is just as true for a cyber force and all can agree that units without effective leadership will not sustain a concerted, competent function in war or in peace.

Next, protection still means the “preservation of the fighting potential of a force so the commander can apply maximum force at the decisive time and place.” [69] To a cyber force, this means that friendly systems and infrastructure must remain uncompromised by outside entities. This may require force, for as the Army so succinctly states, “protection is neither timidity, nor risk avoidance.” [69] Protection minimizes the effects of enemy persistence, payloads, and information, and may include offensive actions to halt enemy activity. To put it another way, as Clausewitz once said: “Even in a defensive position awaiting the enemy assault, our bullets take the offensive. So the defensive form of war is not a simple shield, but a shield made up of well-directed blows.” [12] The Army goes on to say: “These actions conserve the force’s fighting potential so it can be applied at the decisive time and place and incorporates the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy.” [69] With all of the long precedent for offense required to protect oneself from attack, one can see that the current “tying of hands” as regards cyber capabilities is not only unwarranted, but dangerous.

Finally, information also remains much the same. Information “enhances leadership and magnifies the effects of [persistence, payloads, and protection].” [69] Information and intelligence are required if one is to mount effective operations, as it allows leaders to best concentrate persistence and payloads at the decisive place and time. Good situational awareness

and intelligence also allows leaders to make decisions more quickly. For instance, if information about an enemy network has been gathered to include operating systems, patch levels, and installed programs on all connected machines, any order to attack that network could be carried out quickly and easily. Information may also be highly dynamic; a new machine brought online could be in an un-patched state for only a very brief amount of time before it is updated. Information such as this could lead to a decisive decision to install a back door on the target machine for later use. In short, the gathering of information is extremely important in forming a common operational picture and discovering exploitable advantages.

### **Tenets of Cyber Power**

The tenets may remain mostly the same for a Cyber Force, but with one substitution. *Depth* has been replaced with *creativity*, as will be discussed later. First, however, let us discuss *initiative*. Initiative should be important to cyber operations for the same reasons it is on land: it means to “set or dictate the terms of action throughout the battle or operation. Initiative implies an offensive spirit in all operations.” [69] Again, we have a sample of the offensive tone that must also pervade cyber operations. As we have explored earlier, cyber warfare favors the offense, and the current defensive mentality must be changed. Because of this need and the speed at which operations occur, cyber commanders and warriors should have sufficient latitude to take the initiative when opportunities present themselves. It is true that “initiative requires delegating decision making authority to the lowest possible level,” and that in the defense it “implies quickly turning the tables on the attacker... taking aggressive action and... continuing to seek offensive opportunities.” [69] On land, this mentality exists because the lives of our soldiers are of the utmost importance (the Army’s most precious resource). It should exist in a cyber force because our nation’s computer systems and cyberspace infrastructure are also of the

utmost importance; attacks against them need to be taken more seriously. We do not tolerate incursions into our sovereign airspace, land boundaries, or maritime zones; we should approach cyberspace with the same defensive mentality.

Second, agility means the ability to adjust to changing situations quickly and easily. A cyber force should be able to shift targets, objectives, missions, or even types of operations at a moment's notice without confusion or wasted effort. "Agility requires that subordinates act to achieve the commander's intent and fight through any obstacle to accomplish the mission." [69] Agility is doubly important to a cyber force because of the speed at which operations, and therefore changing conditions, may occur. This tenet underscores the need for initiative.

Third, creativity has replaced depth as a tenet for a possible cyber force. To the Army, depth means attacking an enemy all throughout the area of operations in order to deny him freedom to maneuver, thereby affording yourself more space, time, and resources to achieve and exploit success. [69] This is consistent with the use of John Warden's theory for strategic air attack which emphasizes parallel attacks against key operational and strategic nodes. [82] Since there is no maneuver (in a physical sense) in cyberspace, attacking the enemy all throughout an area of operations does nothing more than what occurs when the fourth tenet, synchronization, is applied. Therefore, depth has been replaced with something that will more readily serve a cyber force: creativity. Creativity is necessary in a force where every situation is different and there are no technical orders, field manuals, or checklists to tell a soldier how to proceed. Creativity enhances initiative and agility by exposing opportunities that may have otherwise gone unnoticed. Creativity serves the same purpose as depth in the cyber realm, as it affords the more creative force greater time and resources (space has no corollary) to achieve and exploit success.

Additionally, it works hand in hand with all of the cyber elements of combat power and bolsters the effects of persistence, payloads, leadership, protection, and information.

Next, synchronization remains relatively unchanged and means the “arranging of activities in time, space, and purpose to mass maximum relative combat power at a decisive place and time.” [69] This is just as important to a cyber force, for many reasons. For example, there may be multiple redundant systems operating an enemy asset that a combatant commander wishes disabled, information that allied forces want destroyed may reside on several backup servers, or portions of infrastructure may need to go down at the same time a Special Forces operation is infiltrating an area of enemy territory. Any of the positive results attributed to the omitted depth tenet that a cyber force needs to retain fit here, as synchronization is much the same principle but without the “denial of maneuver” element. Synchronous attacks launched from stationary nodes in cyberspace can quickly overwhelm, overload, subvert, or destroy a great number of enemy systems across an area of operations simultaneously.

Finally, versatility is kept nearly identical. “Competence in a variety of missions and skills allows [cyber] forces to quickly transition from one type of operation to another with [zero] change in force structure. Versatility depends on adaptive leaders; competent, [educated], and dedicated soldiers; and well-equipped units. Effective training, high standards, and detailed planning also contribute.” [69] One of the nice things about cyberspace is the adage “bits is bits” —the flow of traffic through a network is the same, regardless of what the network is for (administrative support, command and control, logistics, etc.). The same knowledge that gets you through an enemy’s defenses can help you bolster your own. Therefore, trained operators can just as easily conduct offensive operations as they can conduct informational ones, etcetera. This lends a high degree of versatility to cyber power.

## Cyber Operations

Of course it's no good having a powerful force if you don't use it to accomplish things. Using the Army's model as a starting point, the four types of cyber operations are offense, defense, inform, and support. First, offensive operations "seek to seize, retain, and exploit the initiative to defeat the enemy decisively." [69] This fits well with our Clausewitzian lessons from earlier; that the purpose of war is always to defeat the enemy. [12] Operationally, this means to directly or indirectly attack the enemy's center of gravity and ultimately to make him concede to your demands. Tactically, defeating the enemy ensures interim or supporting objectives are achieved which make attacking centers of gravity easier. In cyber warfare, offensive operations can take many forms: network attack, electronic attack, kinetic strikes, or some combination of these. The warfighter has all of these options and more when deciding how best to defeat the enemy and create the desired effect in and from cyberspace.

The purpose of defensive operations in any domain is to defeat enemy attacks. It is interesting to note, however, what the Army has to say about defense just because it bears so little resemblance to what we have traditionally done as defense in cyberspace:

*Army forces defend until they gain sufficient strength to attack. Defensive operations defeat an enemy attack, buy time, economize forces, or develop conditions favorable for offensive operations. Alone, defensive operations normally cannot achieve a decision. Their purpose is to create conditions for a counteroffensive that allows Army forces to regain the initiative. Although offensive operations are usually required to achieve decisive results, it is often necessary, even advisable at times, to defend. Commanders defend to buy time, hold terrain, facilitate other operations, preoccupy the enemy, or erode enemy resources. [69]*

Let's break this down into ideas we *cannot* apply to a cyber force:

1. Defending in cyberspace will not provide more strength. Focusing on defense comes at the expense of bleeding away energy and resources because we are always reacting to the adversary's actions. It is possible that our strength might even erode over time.



2. Defensive operations in cyberspace do not buy you time. Cyberspace is a contested domain, 24 hours a day, 7 days a week, 365 days a year. Adversaries attack and probe our defenses at the time and place of their choosing. Countering and responding to these attacks does not delay, hinder, or dissuade further attacks.
3. For the same reasons as cited above, defensive operations in cyberspace also do not economize forces or develop conditions favorable for offensive operations.

And to those we *can* apply to a cyber force:

1. Defensive operations defeat enemy attacks. This is given, but in cyberspace it takes on even more significance. Since nodes of cyberspace may also be centers of gravity, allowing the enemy to compromise them even once could be fatal.
2. Defensive operations normally cannot achieve a decision. As we have discussed earlier, destroying the machines that an attack is coming from will barely slow down the attacks. Cyber warfare favors the offense.
3. Commanders may defend to hold “terrain” and preoccupy the enemy. Keeping enemy hackers out of friendly nodes preserves their computational power for the allied commander. A system that has been compromised by the enemy can in turn be used to launch other attacks; it also undermines trust in the cyberspace infrastructure at large. Deceptive measures—such as appearing to strongly defend a fake network —can divert an enemy away from attacking truly important systems or machines.

Applying land domain doctrine to cyberspace, we see that “successful defenses are aggressive... they maximize [payloads], protection, [and persistence] to defeat enemy forces.” [69]

The *stability operations* function has been replaced by operations to *inform* as a cyber force will have very few actual “boots on the ground.” The contribution of this type of operation

is to inform a nation's populace, and by so doing provide the exact same service as the Army's stability operations: namely, to "promote and protect US national interests by influencing the threat, political, and information dimensions of the operational environment." [69] In an informational operation, cyber forces will see to it that allied messages are placed on electronic media they are able to influence such as radio signals, television broadcasts, web servers, and more. Key information or disinformation may influence said three dimensions of an operational environment. Disheartening enemy combatants, false intelligence for enemy leaders, and truth to dispel propaganda for civilians in enemy territory are examples which may serve to do just that.

Finally, *support operations* have a slightly different meaning to a cyber force. For the Army they mean "assisting civil authorities, foreign or domestic, as they prepare for or respond to crises and relieve suffering." [69] To a cyber force it means to support ongoing friendly operations in all domains. In either case, the purpose of support operations is still to "meet the immediate needs of designated groups for a limited time" [69]; it's just the groups and the needs that change. Some examples of cyber support operations could be the provision of communications or intelligence to forward operating Special Forces operatives, disruption of enemy command and control before the Marines invade a city, or the disabling of integrated air defense nodes before an allied air strike. Cyber support operations may also be useful in peacetime, such as for providing communications to rescue personnel after a natural disaster has destroyed a city's infrastructure.

### **Propositions Regarding Cyber Warfare**

Now that we have defined the elements of cyber power and focused them with tenets that combine to bring power to bear in several kinds of operations, let's take a moment to iterate the

pertinent warfighting characteristics that manifest as a result of the nature of the environment a cyber force operates in. These are:

- Cyber warfare is asymmetric
- Cyber warfare enjoys increasing effectiveness against actors with increasing degrees of technological advancement
- Cyber warfare favors the offense
- Cyber warfare is direct in nature, unless used in a supporting role
- Cyber warfare does not favor position or geography; the terrain is uniform
- Cyber warfare occurs at a tempo much higher than traditional forms of warfare
- Cyber warfare concepts of maneuver and retreat are completely different
- Cyber warfare alone cannot win wars unless total war is acceptable

With these eight propositions, it is now possible to answer the question: what does it take to be powerful in cyberspace? These points will be covered below.

*Cyber warfare is asymmetric.* That is, the cost of entry in terms of both wealth and knowledge needed in order to perform attacks in cyberspace is far below the cost to defend against such attacks. It is also asymmetric in that the importance of the machines being attacked is far greater than the machines doing the attacking. A \$200 dollar laptop with a pirated copy of Windows OS installed on it attacking a financial system worth trillions of dollars is the ultimate in asymmetry. If the attacking machine is destroyed, stolen or lost, the perpetrator buys a new one. The financial system, on the other hand, is much more difficult to replace, which is why risk mitigation strategies such as backups and fault-tolerant systems are employed (which in turn increases the total cost of ownership).

*“Military analysts say that the Chinese know their armed forces cannot match America’s in a head-on confrontation, and they realize their nuclear arsenal pales in comparison.*

*These imbalances have forced Chinese military planners to adopt what the Pentagon calls “asymmetric” techniques—tactics that aim at a foe’s vulnerabilities—in order to counter, or at least deter, U.S. military power.” [32]*

*“The next kind of warfare will be asymmetric warfare. Who is going to take on the United States Army, Marine Corps, U.S. Air Force, and U.S. Navy as probably the most powerful force on the face of the planet?” [41]*

*Cyber warfare enjoys increasing effectiveness against actors with increasing degrees of technological advancement.* It is assumed that technologically advanced societies are also dependent on that technology, which in turn means the society is more affected by the denial or destruction of that technology. A full-scale cyber attack against Afghanistan or Tanzania would largely be an exercise in futility, because these regions are extremely low-tech, with very little in the way of networked machines to disrupt. [24] The attack would be barely noticed, whereas in a nation such as Estonia it could be debilitating [43].

*Cyber warfare favors the offense.* Because networks are first and foremost a means of communicating commands between machines, in order to be useful they must be connected and operational. Additionally, with the technology of the day, their logical location (IP address) rarely changes. This allows attackers to know exactly where target systems are located at all times and to know that said systems will always attempt to process any malicious logic sent to it by the attacker. A determined adversary may “jiggle the doorknobs” and “beat at the doors” indefinitely unless the system in question is disconnected, which defeats the purpose of having it networked in the first place.

*Cyber warfare is direct in nature, unless used in a supporting role.* Unlike warfare in the physical domains, there is no benefit to an indirect approach in cyberspace. The enemy knows where your networks are; you know where your enemy’s networks are; both you and your enemy’s networks are available to be attacked at any time. There is no need for feints,

subterfuge, diversions, or deception: If you want to attack a certain target, there is nothing stopping you from going straight at it. You either succeed or fail in the attack. The caveat to this is that when cyber power is used in a *supporting* role, it can most certainly be used indirectly, and to great effect. Examples of this would be using Information Operations to “leak” some information onto a blog about an invasion that is supposed to be taking place in one location when it is really taking place in another, or by using electronic warfare (jamming) to degrade radar coverage in one sector of the enemy’s air defense to make them believe an attack is coming from that direction when in reality a B-2 is stealthily winging its way to a different target in another location.

*Cyber warfare does not favor position or geography; the terrain is uniform.* In this context, terrain refers to the networking terrain, such as the connections, the networking protocols and means of data transmission. In this way, it is very similar to the domains of Sea, Air, and Space. In the maritime environment, water is water and ships maneuver and float (Archimedes’ principle of buoyancy and displacement) the same whether they are in the Pacific or Atlantic or Mediterranean. The same holds true for air (Bernoulli’s principle and lift) and space (Kepler’s laws of planetary motion). Cyberspace is the same. Electromagnetic energy propagates through free space in a standard manner, and internet protocol networks function in a consistent way. With that said, there is a significant difference between cyberspace and the other domains. While the mechanics of energy and information transfer in cyberspace are standard, cyberspace is constructed by humans, in that we use the standards and equipment to connect and build cyberspace. In other words, we “build” and shape terrain when new networks are formed or reconfigured. But the flow of information through the networks is well understood and predictable.

*Cyber warfare occurs at a tempo much higher than traditional forms of warfare.*

Because humans can never react in time to counter the first salvoes of a cyber attack, much of the responses to an attack must be automated. The situation after the initial attack may also begin to change and deteriorate extremely rapidly. Swift action needs to be undertaken to prevent further harm, either by means of a counterattack (ideally) or isolation (undesirably). Blocking the attacker may work depending upon the adversaries' expertise – if IP's from multiple or unlimited different subnets are coming at you and blocking is impossible, isolation may be preferable to compromise or destruction.

*Cyber warfare concepts of maneuver and retreat are completely different.* With current levels of technology, nodes within cyberspace are logically stationary. There is no “high ground” to rain blows upon your enemy from; no narrow defile with which to hold off a force five times your size for months; no swamp to lead them into in order to bog them down (note that honeynets would not be a form of maneuver as some have suggested—IP addresses are still as of yet static—but a form of deception, like the building of wooden airplanes in WWII). If an enemy is pressing you hard, you cannot withdraw your forces back over the last ridge to rest and regroup; your firewall must remain where it is, taking on wave after wave of attack to protect your intranet from compromise until either the attacker stops, is destroyed, or successfully defeats your defenses. In this way, combat in the cyber domain is much like the trench warfare of WWI, with your local area networks being your trench and the World Wide Web as no-man's land.

Lastly, *cyber warfare alone cannot win wars unless total war is acceptable.* Total war encompasses attacks against your enemy's populace. In order to cause enough damage to a nation to force capitulation to your demands, any cyber attack would invariably affect the

civilian population of the target nation to its extreme detriment. Because a large percentage of cyberspace exists within commercial, civilian infrastructure, unrestrained cyber warfare “could, in fact, be in the magnitude of a weapon of mass destruction.” [32] Attacks against financial targets, electrical power grids, national leadership and government structures, etc. are all potentially valid targets (and legitimate under the laws of war); however, commanders must assess whether the second and third order effects of attacking these targets is acceptable.

So now back to our original question. What does it take to be powerful in cyberspace? The Air Force believes that the control of an environment, be it air, space, or cyberspace, means to assure the friendly use of that environment while denying its use to an enemy. [65] While this is true, it is doubtful that a force will ever be able to completely deny the use of cyberspace to an enemy; however, one becomes powerful by acknowledging the above eight propositions and working to either mitigate or embrace each one and not try to ignore them or operate contrary to them.

- A nation wishing to be powerful in cyberspace will mitigate the asymmetry of cyber warfare by increasing the cost of entry needed to oppose them. This can be accomplished in a number of ways. Examples include using secure, proprietary operating systems, hard and software that is not known by or accessible to bad actors. Ironically, this is exactly opposite to recent trends in which government, military, and critical infrastructure systems have become increasingly based on commercial off the shelf (COTS) technology, largely to reduce operations and maintenance costs. Investing in “closed” technology would prevent attackers from using widespread and freely available exploits that are common to most commercial software. Another example would be diversification, which is also contrary to recent trends in adopting a homogeneous

environment based on a single technology, such as Microsoft Windows. Diversification forces an adversary to become proficient in more than one type of technology, which would in turn slow them down.

- A nation wishing to be powerful in cyberspace must also mitigate the inordinate amount of damage that a less technologically advanced actor may perpetrate. This may be accomplished by ensuring that all security elements are placed out of band of operating systems, sensitive information, intellectual property, and etcetera. In this way, an attacker may not leverage flaws in logic to corrupt, disrupt, or exploit critical data.
- In order for a nation to be powerful in cyberspace, it must embrace the fact that cyber warfare favors the offense. Our current approach to cyberspace defense is not a strategy for winning in cyberspace...it only drains resources, and despite the tremendous advancements in security technology, we continue to fall behind, because new exploits and vulnerabilities continue to appear. A different approach is required. It must take the offense at all times, attacking its enemy ruthlessly even in the defense. It must recognize that destruction of the enemy is the only way to end a cyber attack. There is nothing to be gained in absorbing blows.
- A powerful nation will embrace the direct nature of cyber combat. If a commander wants a certain system taken offline, he should order that system attacked. Feinting at a different target will not decrease the protections on the actual target (as an enemies cyber defenses should always—except through mistake or incompetence—be at the maximum level at any given time), and will only decrease resources that could be better employed elsewhere.



- A powerful nation will embrace the uniformity of the terrain and seek intimate knowledge as to the nature of electromagnetism. It will use this knowledge to develop weapons and techniques for disrupting, manipulating, and intercepting enemy signals, while likewise developing technology which assures the integrity, confidentiality, and availability of its own electromagnetic transmissions.
- A nation wishing to be powerful in cyberspace should both embrace and act to mitigate the double-edged sword of extremely high-tempo operations. In the former, it will use this speed in maneuver operations designed to strike numerous targets in the heart of enemy territory, overwhelming the opponent's OODA loop and thereby disorienting him and causing chaos or collapse. In the latter, a powerful cyber force should lessen the impact of these tremendous speeds by employing autonomic defense/react protections and by delegating authority to respond to the lowest possible level.

*Given the speed with which data or information moves in cyberspace, the decision cycle during an operation may be compressed to seconds or milliseconds. This characteristic of the domain requires the generation of predetermined or automated responses to potential cyberspace attacks. Additionally, the compressed decision cycle requires predetermined rules for intelligence, surveillance, and reconnaissance (ISR) actions that enable counterattacks against time-sensitive and fleeting targets. This places a premium on IPOE needed for pre-planning. In cyberspace, responses to enemy actions take milliseconds versus traditional joint air operations planning timelines. Therefore, prior planning is necessary for success of both offensive and defensive operations to ensure our freedom of action. [64]*

- In order for a nation to be powerful in cyberspace, it will mitigate the lack of maneuver or retreat by employing redundant systems and backing up critical data to multiple locations. If the enemy wins through your defenses and takes down a node, a powerful nation will be able to “fight through” the attack and mitigate it as quickly as possible.

- And finally, a nation wishing to be powerful in cyberspace will embrace the fact that to win a war through cyber power alone, it must be a total war. It will not shrink from necessary but regrettable collateral damage, as anything less than a maximum effort to destroy an enemy's center of gravity within cyberspace (be it financial, economic, or informational) simply cannot cause enough damage to force capitulation. Let us finish by reiterating the wisdom that Clausewitz has given us; "war is an act of force, and there is no logical limit to the application of that force." [12]

Not only will a nation that has taken these eight steps will find itself a very "hard target," but it will also possess the ideology it needs to dominate cyberspace in the 21<sup>st</sup> century. America already possesses the tools; all that remains is for her to prove Mahan wrong by overcoming the inertia of the conservative class and changing her tactics towards war in the cyber domain.

## **V. Conclusions and Recommendations**

### **Research Overview**

The research conducted and explained in this paper had three main objectives, which were discussed in chapter one. Historical accounts have shown that in regard to dominion, much as with nearly everything else in human experience, mastery requires specialization.

Additionally, both historical and contemporary writings indicate that long periods of trial and error have created excellent strategic precedent as to the gaining and wielding of power in each of the known domains. There is great wisdom in admitting that not much comes along within the human experience that is truly new or unique, and that it is therefore possible to learn from past mistakes if only one listens. Finally, a combination of the different services' strategies, both past and present, along with research of contemporary service strategies, was synthesized to create a possible vision of future cyber power.

### **Conclusions and Significance of Research**

Studying the reasons, precedents, history, successes, failures, ideas, and accepted truths in this research concluded that it is necessary to create a separate Cyber Force if the United States wishes mastery over and domination of Cyber Space. It was also determined that some, but not all of the strategic lessons and operating principles of other domains may be applied to aid in the creation of a comprehensive cyber strategy. The rest was synthesized from historic precedent and contemporary research. What coalesced was a strong assertion of principles for mastering the cyber domain which cry out for adoption under a separate cyber service.

### **Recommendations for Future Research**

While this research detailed the differences of environment, and therefore principles and strategy, which necessitate the creation of a separate cyber force, much research still needs to be

accomplished in regard to the four types of operations a cyber force may undertake. How does one predict the yield of payloads? How much persistence is too much? How does one assess damage in cyberspace? How does one measure security? Trust? How much should one spend on protections? How does a military service protect a utility company's servers, or even a private citizen's PC? Should they? How much right to privacy do civilians have in cyberspace if national security is at stake? What constitutes an act of war in cyberspace? The questions are endless, and many good research topics abound.

### **Summary**

Domains are portions of an environment you can exert dominion over. Dominion relies upon strategy. Strategies are shaped by environment. History shows that separate military services are required to master a strategy for each individual environment (and therefore domain), and so every domain a nation wishes to master requires a separate service. These are the lessons we have learned along our journey. So, too have we learned about the differing strategies for environmental dominion held by the great historical military thinkers. We then followed the evolution of their ideas to the modern-day strategies of the current services and applied what we could take from each one, both historic and modern, to the cyber domain and discarded all of the rest. What is left over is an envisioning of the strategy a hypothetical Cyber Force must embrace, both to serve as a strong case for its independence and to successfully wage war in this newest, evolving domain: cyberspace. It is a vision of...

Cyber Power in the 21<sup>st</sup> Century.

## Bibliography

1. 90th Congress of the United States. Treaty 90-8. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies. 10 October 1967. 15 July 2008.  
<<http://www.au.af.mil/au/awc/awcgate/tufts/BH500.htm>>
2. AFCYBER Public Affairs. Air Force Leaders Work to Develop Cyberspace Roadmap. Air Force Cyber Command. 24 Oct 2008. 6 Dec 2008.  
<<http://www.afcyber.af.mil/news/story.asp?id=123121147>>
3. AFCYBER Public Affairs. Fact Sheets: Cyberspace 101. U.S. Air Force. Unknown Date. 11 Dec 2008.  
<<http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10784>>
4. “American Revolution.” Encyclopedia Britannica. Encyclopedia Britannica Online. 2008. 1 July 2008. <<http://www.britannica.com/EBchecked/topic/617805/American-Revolution>>
5. “American Revolution.” Microsoft Encarta Online Encyclopedia. 2008. 27 June 2008.  
<<http://encarta.msn.com>>
6. Boyne, Walter J. Beyond the Wild Blue. St. Martin’s Press, New York, NY. 1997.
7. Brewin, Bob. “Battlespace.” What’s Brewin’: Inside Defense Information Technology. Government Executive. 13 Oct 2008. 6 Dec 2008.  
<<http://www.govexec.com/dailyfed/1008/101308wb.htm>>
8. Builder, Carl H. The Masks of War: American Military Styles in Strategy and Analysis. The Johns Hopkins University Press. Baltimore, MD. 1 Feb 1989.
9. Burlingame, Roger. General Billy Mitchell: Champion of Air Defense. McGraw-Hill Book Company, Inc, New York, NY. 1953.
10. Buzanowski, J. G. Cyberspace Expert Briefs AFA Conference Attendees. Secretary of the Air Force Public Affairs. 9/27/2007. 23 Aug 2008.  
<<http://www.af.mil/news/story.asp?id=123069727>>
11. Chavanne, Bettina H. “New Cyber, Electronic Weapons Slow.” Aviation Week.  
<<http://www.aviationweek.com/aw/blogs/defense/index.jsp>>
12. Clausewitz, Carl von. On War. Princeton University Press. Princeton, NJ. 1989.
13. Convertino, Sebastian, et al. Flying and Fighting in Cyberspace. Air War College, Maxwell AFB, AL. July 2007
14. Dalton, John. Forward ...From the Sea. Department of the Navy. 1994.

15. Department of Defense. Quadrennial Defense Review Report. Office of the Secretary of Defense. Washington, D.C. 6 Feb 2006.
16. Department of the Navy. Naval Doctrine Publication 1: Naval Warfare. Office of the Chief of Naval Operations. Washington, D.C. 28 Mar 1994.
17. Department of the Navy. Naval Historical Center. Commodore Esek Hopkins, Continental Navy, (1718-1802). 14 Dec. 2002. 23 Dec. 2007. <<http://www.history.navy.mil/photos/pers-us/uspers-h/e-hopkns.htm>>
18. Department of the Navy. Naval Historical Center. Navy Birthday Information – 13 October 1775. 4 Oct. 2000. 23 Dec. 2007. <<http://www.history.navy.mil/birthday.htm>>
19. Department of the Navy. Naval Historical Center. The Pearl Harbor Attack, 7 December 1941. 31 Jan 2008. 7 Jul 2008. <<http://history.navy.mil/faqs/faq66-1.htm>>
20. Department of the Navy. NETWARCOM Mission Statement. Naval Network Warfare Command. Unknown date. 6 Dec 2008. <<http://www.netwarcom.navy.mil/about-us/mission.htm>>
21. “domain.” Merriam-Webster Online. Merriam-Webster, Inc. Jul 2008. <<http://www.merriam-webster.com/dictionary/domain>>
22. Donley, Michael B. and Norton A. Schwartz. SECAF/CSAF Letter to Airmen: Mission Statement and Priorities. Office of the Secretary of the Air Force. 15 Sep 2008.
23. Douhet, Giulio. The Command of the Air. Coward-McCann, Inc. New York, NY. 1942.
24. Dunlap, Charles J. “How We Lost the High-Tech War of 2007: A Warning from the Future.” The Weekly Standard. 29 Jan 1996.
25. Echevarria, Antulio J. Clausewitz’s Center of Gravity: Changing our Warfighting Doctrine—Again! Strategic Studies Institute. Carlisle, PA. September 2002.
26. England, Gordon. Memorandum for Secretaries of the Military Departments. The Definition of “Cyberspace.” 12 May 2008.
27. Executive Office of the President. National Strategy for Combating Terrorism. Office of Homeland Security. Washington, D.C. 2006. <<http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf>>
28. Executive Office of the President. The National Strategy to Secure Cyberspace. Office of Homeland Security. Washington, D.C. February 2003.

29. France, Martin E.B. Back to the Future: Space Power Theory and A.T. Mahan. Air & Space Power Journal. 4 August 2000.
30. Fritz, Jason. “How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness.” Culture Mandala. Vol. 8, No. 1. October 2008.
31. Graff, David and Robin Higham. A Military History of China. Westview Press. Jackson, TN. March 2002.
32. Harris, Shane. “China’s Cyber-Militia.” National Journal Magazine. 31 May 2008. <[http://www.nationaljournal.com/njmagazine/cs\\_20080531\\_6948.php](http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php)>
33. Haynal, Russ. Internet Growth Charts. Information Navigators. 26 Oct 2006. 17 July 2008. <<http://navigators.com/stats.html>>
34. Hurley, Alfred. Billy Mitchell: Crusader for Air Power. Indiana University Press, Bloomington, IN. 1964.
35. Jones, Johnny R. William “Billy” Mitchell’s Air Power. Airpower Research Institute. September, 1997.
36. Krebs, Brian. “Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.” Washington Post Online. 16 Oct 2008. 7 Dec 2008. <[http://voices.washingtonpost.com/securityfix/2008/10/report\\_russian\\_hacker\\_forums\\_f.html](http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html)>
37. Kristula, Dave. The History of the Internet. March 1997. 17 July 2008. <<http://www.davesite.com/webstation/net-history.shtml>>
38. Kuehl, Dan. Cyberspace – Cyberpower: Their Influence on (Future) History (DRAFT). National Defense University. November, 2008.
39. Levine, Henry. “US-China: The Threat of Economic MAD.” Hedging Against Uncertainty: US Strategy in an Interdependent World. National Strategy Forum. Vol. 17, No. 3. Summer 2008. <<http://www.nationalstrategy.com/Programs/NationalStrategyForumReview/NationalStrategyForumReviewSummer2008/USChinaThreatofEconomicMADNSFRSummer2008/tabid/161/Default.aspx>>
40. Levine, Isaac. Mitchell: Pioneer of Air Power. Duell, Sloan, and Pearce. New York, NY. 1943.
41. Lord, William. Military Fellows Roundtable: Air Force Cyberspace Command: Protecting Against an Electronic Pearl Harbor. Remarks to the Council on Foreign Relations. Washington, D.C. 31 Mar 2008.

42. Mahan, Alfred T. The Influence of Sea Power Upon History, 1660-1783. Little, Brown and Company. Boston, MA. 1918.
43. McAfee Corporation. McAfee Virtual Criminology Report. 2007. <[www.mcafee.com/us/](http://www.mcafee.com/us/)>
44. Mitchell, Ruth. My Brother Bill. Harcourt, Brace and Company, New York, NY, 1953.
45. Mitchell, William. Our Air Force. E. P. Dutton & Co. New York, NY. 1921.
46. Mitchell, William. "Aeronautical Era." The Saturday Evening Post. Curtis Publishing Company. Philadelphia, PA. December 20, 1924
47. Mitchell, William. Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military. Dover Publications. Mineola, NY. 5 May 2006.
48. Mitnik, Kevin D. The Art of Intrusion. John Wiley & Sons. Hoboken, NJ. 4 March, 2005.
49. Moore, Ronald D. Battlestar Galactica; Season 1-3. Universal Studios, 20 September 2005.
50. Moseley, T. Michael. Operational Cyberspace Command "Go Do" Letter. 01 Nov 2006.
51. Moseley, Michael T. "The Nation's Guardians: America's 21<sup>st</sup> Century Air Force." CSAF White Paper. 29 Dec 2007.
52. Mostow, Jonathan. Terminator 3: Rise of the Machines. Warner Home Video, 2 July 2003.
53. Nalty, Bernard C. Winged Shield, Winged Sword. Air Force History and Museums Program. Washington, D.C. 1997.
54. National Aeronautics and Space Administration. National Space Science Data Center. Sputnik 1. 2 April 2008. 14 July 2008. <<http://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.od?id=1957-001B>>
55. National Maritime Museum. Ships, Seafarers, and Life at Sea. 2008. 26 Jun 2008. <<http://nmm.ac.uk/server/show/conWebDoc.168>>
56. Offner, Jim. "E-Commerce to Ring Up 17 Percent Growth in '08." E-Commerce Times. 08 April 2008. 26 Aug 2008. <<http://www.ecommercetimes.com/story/62494/html>>
57. Past Presidents. "George Washington." The White House. 1 July 2008 <<http://www.whitehouse.gov/history/presidents/gw1.html>>



58. Pike, John. B-2 Spirit. Federation of American Scientists: The Nuclear Information Project. 30 Nov 1999. Oct 2008.  
<<http://www.fas.org/nuke/guide/usa/bomber/b-2.htm>>
59. “power.” Merriam-Webster Collegiate Dictionary, 11<sup>th</sup> ed. Miriam-Webster. Springfield, MA. April 2006
60. Schlaikjer, Erica. Internet Evolution: China’s Youth Culture Grows Up in Cyberspace. The Abroad View Foundation. 2008. 12 Sep 2008,  
<<http://www.abroadview.org/asia/schlaikjer.htm>>
61. Stephens, Hampton. “War in the Third Domain.” Air Force Magazine Online. April, 2007: Vol. 90, No 4.  
<<http://www.airforcemagazine.com/MagazineArchive/Pages/2007/April%202007/0407war.aspx>>
62. Tzu, Sun. The Art of War. Basic Books. New York, NY. 10 Feb 1994
63. United States Air Force. Air Force Doctrine Document 1, Air Force Basic Doctrine. Air Force Doctrine Center, Maxwell AFB, AL. 17 Nov 2003.
64. United States Air Force. Air Force Doctrine Document 2-X (DRAFT), Cyberspace Operations. Air Force Doctrine Center, Maxwell AFB, AL. 4 Feb 2008.
65. United States Air Force. Air Force Manual 1-1, Basic Aerospace Doctrine of the United States Air Force. Air Force Doctrine Center, Maxwell AFB, AL. March 1992
66. United States Air Force. National Museum of the Air Force. The First Flight. Unknown Date. 27 Dec 2007.  
<<http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=658>>
67. United States Air Force. Strategic Vision. Air Force Cyber Command. 3 Mar 2008.  
<<http://www.afcyber.af.mil/shared/media/document/AFD-080303-054.pdf>>
68. United States Army. 1<sup>st</sup> Information Operations Command (Land). Intelligence and Security Command (INSCOM). Unknown date. 6 Dec 2008.  
<<http://www.inscom.army.mil/MS/Default1st.aspx?text=off&size=12pt>>
69. United States Army. Field Manual 3-0, Operations. Headquarters, Department of the Army. Washington, D.C. 14 June 2001
70. University of Pennsylvania. The ENIAC Museum Online. 23 Apr 2003. 27 Jan 2008. <<http://www.seas.upenn.edu/~museum/>>

71. U.S. Centennial of Flight Commission. Balloons in the American Civil War. Unknown Date. 26 Dec 2007. <[http://www.centennialofflight.gov/essay/Lighter\\_than\\_air/Civil\\_War\\_balloons/LTA5.htm](http://www.centennialofflight.gov/essay/Lighter_than_air/Civil_War_balloons/LTA5.htm)>
72. U.S. Centennial of Flight Commission. Military Use of Balloons During the Napoleonic Era. Unknown Date. 26 Dec 2007. <[http://www.centennialofflight.gov/essay/Lighter\\_than\\_air/Napoleon%27s\\_wars/LTA3.htm](http://www.centennialofflight.gov/essay/Lighter_than_air/Napoleon%27s_wars/LTA3.htm)>
73. U.S. Joint Chiefs of Staff. Joint Net-Centric Operations Campaign Plan. Command, Control, Communications, and Computer Systems Directorate (J6). October 2006.
74. U.S. Joint Chiefs of Staff. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. J-7 Joint Education and Doctrine Division. 17 Oct 2008.
75. U.S. Joint Chiefs of Staff. Joint Publication 3-0, Joint Operations. J-7 Joint Education and Doctrine Division. 13 Feb 2008.
76. U.S. Joint Chiefs of Staff. Joint Publication 3-13, Information Operations. J-7 Joint Education and Doctrine Division. 13 Feb 2006
77. U.S. Joint Chiefs of Staff. Joint Publication 3-14, Joint Doctrine for Space Operations. J-7 Joint Education and Doctrine Division. 9 Aug 2002
78. U.S. Joint Chiefs of Staff. Joint Publication 5-0, Joint Operation Planning. J-7 Joint Education and Doctrine Division. 26 Dec 2006.
79. U.S. Joint Chiefs of Staff. The National Military Strategy of the United States of America. Washington, D.C. 2004
80. U.S. Joint Chiefs of Staff. The National Military Strategy for Cyberspace Operations. Office of the Chairman of the Joint Chiefs of Staff. Washington, D.C. December 2006.
81. Verstappen, Stefan H. The Thirty-Six Strategies of Ancient China. China Books & Periodicals Inc. San Francisco, CA. 30 Jan 1999.
82. Warden, John A. "Air Theory for the 21<sup>st</sup> Century." Battlefield of the Future: 21<sup>st</sup> Century Warfare Issues. Air University. September 1995. 11 Dec 2008. <<http://www.airpower.maxwell.af.mil/airchronicles/battle/chp4.html>>
83. War Department. Field Manual 100-20, Command and Employment of Air Power. United States Government Printing Office, Washington, D.C. 21 July, 1943.
84. Wright, Robert. The Continental Army. Washington, D.C.: Center of Military History, 1983.

85. Wynne, Michael W. Cyberspace as a Domain in Which the Air Force Flies and Fights. Remarks as delivered to the C4ISR Integration Conference. Crystal City, VA. 2 Nov 2006.
86. Wynne, Michael W. and T. Michael Moseley. SECAF/CSAF Letter to Airmen: Mission Statement. Office of the Secretary of the Air Force. 17 Dec 2005.
87. “Cyberspace.” Instructor Presentation: Defining Cyberspace. AFIT CSCE-525. July 2007. July 2007.
88. “Network Map.” Teleglobe Communications Corporation. Mumbai, India. Nov 1999. 19 September 2008.  
<[http://www.teleglobe.com/en/our\\_network/](http://www.teleglobe.com/en/our_network/)>
89. “In-Service Plan.” The Williams Companies, Inc. Tallahassee, FL. January 2000. 19 September 2008.  
<<http://www.williamscommunications.com>>
90. “Telstar 5.” Loral Skynet, Inc. Gloucester, ON. February 2007. 19 September 2008.  
<<http://www.loralskynet.com>>

## Vita

Joseph Elbaum is a former USAF Communications and Information officer currently finishing his Masters in Cyber Operations under the CyberCorps' Scholarship for Service program. Following his graduation, he will utilize his abilities as an Information Security Officer with a government agency.

## REPORT DOCUMENTATION PAGE

*Form Approved*  
*OMB No. 074-0188*

The 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 the collection of information. Send comments regarding this burden estimate or any other aspect of the 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 a 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.**

<b>1. REPORT DATE (DD-MM-YYYY)</b> 18-12-2008		<b>2. REPORT TYPE</b> Master's Graduate Thesis		<b>3. DATES COVERED (From - To)</b> May 2007 - Dec 2008	
<b>4. TITLE AND SUBTITLE</b>  CYBER POWER IN THE 21ST CENTURY			<b>5a. CONTRACT NUMBER</b>		
			<b>5b. GRANT NUMBER</b>		
			<b>5c. PROGRAM ELEMENT NUMBER</b>		
<b>6. AUTHOR(S)</b>  Joseph M. Elbaum, AD-21, USAF			<b>5d. PROJECT NUMBER</b>		
			<b>5e. TASK NUMBER</b>		
			<b>5f. WORK UNIT NUMBER</b>		
<b>7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)</b> Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765				<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>  AFIT/GCO/ENG/09-01	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> This space intentionally left blank				<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>	
				<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>	
<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b> APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.					
<b>13. SUPPLEMENTARY NOTES</b>					
<b>14. ABSTRACT</b> Historically, the United States Congress has acknowledged that a separate branch of military service is required to exert supremacy over each of the recognized Domains of Operation. Throughout the evolution of modern warfare, leading minds in military theory have come to the conclusion that due to fundamental differences inherent in the theory and tactics that must be employed in order to successfully wage war within a domain's associated environment, a specialized force was needed - until now. With the recent inclusion of Cyberspace as an operational domain by the Department of Defense, the case should be made that it, too, is far too specialized an area to be rolled up into any or all of the current branches of service.  This research investigated the concept of cyber power in the 21st century, what it means to wield it, and how this capability may be used to wage war. It argues that cyberspace as a domain should be treated no differently than the traditional warfighting domains: that it, too, is an arena where defense may best be secured by attacking the enemy, where battles occur for control of territory, where denial affects combat in other domains, and where political motives dictate the course of hostilities. Because the strategic challenges and concepts are the same and yet the environment so specialized, the research concludes that the only way to properly secure the domain and to prosecute war effectively is to create a U.S. Cyber Force.					
<b>15. SUBJECT TERMS</b> Cyberpower, cyberspace, strategy, doctrine					
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>  UU	<b>18. NUMBER OF PAGES</b>  116	<b>19a. NAME OF RESPONSIBLE PERSON</b> Robert F. Mills, PhD, AFIT/ENG
<b>REPORT</b> U	<b>ABSTRACT</b> U	<b>c. THIS PAGE</b> U			<b>19b. TELEPHONE NUMBER (Include area code)</b> (937) 255-3636 x4527 (DSN 785-), robert.mills@afit.edu