REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
24-04-2015	Master of Military Studies Research Paper	September 2014 - April 2015

4. TITLE AND SUBTITLE

Cyber and the Myth of the Bloodless Battlefield:
The Cyber Domain Supporting a Combined Arms Fight

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Kukla, Jennifer A., Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

The attitude toward cyber warfare today is parallel to that of air warfare a century ago. The tone of scholarly writing on cyber is reminiscent of the theories touted by Giulio Douhet in the early 20th century. Many of Douhet's theories were disproven over time. We should look to history for examples of both fear and sensationalism in the perceived threats posed by first generations of new military capabilities. Current theories promoting bloodless cyber warfare will lead us away from the more sound military use of cyber operations as a function of warfare integrated into the traditional kinetic approach.

Current U.S. policy requires presidential approval for military personnel to respond to or execute an attack. This centralized authority will impair the U.S. military's ability to fight future wars effectively. The Marine Corps should begin including cyber operations in training and education of Marines and their leadership. The Marine Corps will be better suited for tomorrow's battlefield if cyber is treated as it should be: another tool available to the commander in a combined arms fight.

15. SUBJECT TERMS

Cyber Warfare; Air Power; Combined Arms; Cyber Domain

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	40	Marine Corps University/Command a
Unclass	Unclass	Unclass			**19b. TELEPHONE NUMBER** *(include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Cyber and the Myth of the Bloodless Battlefield:
The Cyber Domain Supporting a Combined Arms Fight

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Major Jennifer A. Kukla, USMC

AY 14-15

Mentor and Oral Defense Committee Member: Matthew Flynn
Approved: _____
Date: 4/24/15

Oral Defense Committee Member: Hugh Overdorf
Approved: _____
Date: 4/24/15

T.W. Gordon
4/24/15

4/24/15

Executive Summary

Title: Cyber and the Myth of the Bloodless Battlefield: The Cyber Domain Supporting a Combined Arms Fight

Author: Major Jennifer A. Kukla, United States Marine Corps

Thesis: Gains made in cyberspace alone will not be sufficient to achieve victory; therefore a bloodless "cyber war" is not possible and failure to account for operations in all domains will lead to protracted political engagements.

Discussion: Political leaders and scholars alike are buying into the fear and hype surrounding cyber warfare. In keeping with this excitement, the Department of Defense (DoD) has created an entire sub-unified command, U.S. Cyber Command, to partner with the National Security Agency (NSA) and conduct full spectrum military cyberspace operations. The attitude toward cyber warfare today is parallel to that of air warfare a century ago. The tone of scholarly writing on cyber is reminiscent of the theories touted by Giulio Douhet in the early 20th century. Many of Douhet's theories were disproven over time.

The path the DoD has currently set for the implementation of cyber warfare is unsustainable. There will be no magical war fought only in cyberspace by skilled hackers at the NSA and U.S. Cyber Command. Effects from a conflict in cyberspace will be felt in the physical realm, whether through cyber-driven kinetic effects or impacts to the nation's critical infrastructure and economy. In the event of a second-strike scenario, the nation's people and our military will need to respond in both physical space and cyberspace. Thus, a bloodless war fought entirely within cyberspace is not possible. An adversary may desire to restrict the conflict to cyberspace but the victim of the cyber attack will utilize his strengths, which may be kinetic.

Conclusion: Current U.S. policy requires presidential approval for military personnel to respond to or execute an attack. This centralized authority will impair the U.S. military's ability to fight future wars effectively. The Marine Corps should begin including cyber operations in training and education of Marines and their leadership. The Marine Corps will be better suited for tomorrow's battlefield if cyber is treated as it should be: another tool available to the commander in a combined arms fight.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Page

PAGE INTENTIONALLY LEFT BLANK

Preface

The inspiration for this paper was an interest in cyber command prompted by suggestions from senior leadership that I look into finding a home in the cyber world after the retirement of the EA-6B Prowler. My experience in the non-kinetic world of electronic warfare as an Electronic Countermeasures Officer in the EA-6B gives me a unique perspective from which to view the future of cyber warfare and how the Marine Corps can best operate within this new domain.

In the course of my research, I discovered that the Department of Defense, Department of Homeland Security, National Security Agency, and the civilian sector all have differing approaches to the problem of cyber warfare. Each agency has differing motives for getting involved in the fight for cyber dominance, and a struggle exists between the government and civilian cyber security agencies to secure the nation's endeavors in cyberspace.

I would like to thank Colonel Todd Desgrosseilliers and Brigadier General John Simmons both for encouraging me to consider a future in the cyber field, as well as Brigadier General Frank Kelley for opening my eyes to the dynamics within the cyber community and the future of Marine Corps Electronic Warfare. I would also like to thank my dad, Dr. Jon Kukla, for his continued support and constructive feedback on many rough drafts throughout my time at Command and Staff College. Finally, I am grateful to Dr. Matthew Flynn for assuming the role of cyber expert at Command and Staff College, providing thought-provoking discussions on the topic, and direction throughout the writing process.

PAGE INTENTIONALLY LEFT BLANK

Introduction

Since the Internet entered the homes of everyday civilians, societies and nation-states have become increasingly connected. This new interconnected world brings with it not only many advantages but also many risks. Recent cyber events, including the highly publicized hacks into Sony Entertainment and Anthem Healthcare, highlight the vulnerabilities that come with the convenience of an Internet connection. Many experts consider cyber the newest domain of warfare because it permeates nearly everything within Western society and much of the world. With countries increasingly automating their critical infrastructure, failure to properly defend those networks could result in disaster.

This forecast hanging over this early age of information warfare in cyberspace is strikingly similar to the introduction of warfare in the air domain. Politicians, military leaders, corporate leaders, and theorists alike recognize the capabilities of cyber as a weapon. Their analysis mirrors those who once struggled with discerning the application of aircraft to the battlefield. Yet, there are still many lingering questions about this new battlefield. What is cyber warfare? What is the difference between cyber attack and cyber sabotage? Is it possible to wage a war completely within the cyber realm and avoid bloodshed? Hollywood and the entertainment industry have been exploring this in the fictional realm for decades in movies like *Live Free or Die Hard* (2007), *The Net* (1992), and *WarGames* (1983).[*] It is time for the Department of Defense (DoD) to determine how the nation will handle these scenarios when they are no longer confined to the movie screen.

The following analysis advances this process for the DoD by exploring similarities between the beliefs of airpower theorists of the 19th century and those of cyber theorists of today.

[*] In *Live Free of Die Hard*, hackers target the US computer infrastructure, crash the stock market, and cripple the economy. In *The Net*, the main character discovers a conspiracy involving prominent cyber security company. In *WarGames*, a kid hacks into the computers that control the U.S. nuclear arsenal.

With this historical perspective, one is able to conclude that cyber (like airpower) is not a new frontier on which the battles of the future will be fought but rather another aspect of warfare that the commander must consider in his or her combined arms approach. In this paper I will explore whether governments, through the sole use of the cyber domain, can effectively break the will of an enemy. To do this, I will rely on historical examples of military thought at the establishment of new warfare domains, specifically the air domain, and how those theories have or have not stood the test of time. I will also study examples of cyber "attacks" and discuss whether those meet the criteria to be acts of war. When this insight is offered, the cyber world as a battlefield, and one divorced from its civilian recreational users, comes to the fore as a key area in need of understanding. What is most valuable to understand is that gains made in cyberspace alone will not be sufficient to achieve victory; therefore a bloodless cyber war is not possible and failure to account for operations in all domains will lead to protracted political engagements.

Literature Review

The amount of literature available on the role cyber will play in determining the outcome of future conflicts is growing, but it remains in a state of underdevelopment given the newness of cyber. When studying this domain of warfare in an unclassified setting, the most current theories strive to offer a greater understanding of the problem. They succeed, in part. For example, in *@ War: The Rise of the Military-Internet Complex,* published in November 2014, Shane Harris offers a current, comprehensive assessment of the known uses of cyber in recent conflicts and the conflict between the government and civilian sectors regarding the classification of cyber threats. Harris refers to some examples as sabotage, others as espionage, and still others as acts of war; he stops short of explaining the difference between the three in a definitive way.[1] This shortcoming is in keeping with recently published government documents, from the 2013 "Executive Order on Improving Critical Infrastructure Cybersecurity," to the 2011 "International Strategy for Cyberspace," to the 2009 "Cyberspace Policy Review," to the 2008 "Comprehensive National Cybersecurity Initiative." None of these government documents defines terms like cyber attack or cyber warfare, an omission of somewhat startling proportions.

The lack of definition limits the researcher and theorist, both past and present, in terms of determining what constitutes a cyber war, whether it is possible, and what it would look like. There are many doomsday writers out there who anticipate cyber attacks as threats to national security that could cripple the nation.[2] Even high-ranking politicians have bought into this hype. In 2012, former Defense Secretary Leon E. Panetta warned of a "cyber-Pearl Harbor." [3] Later, in 2013, former Homeland Security Secretary Janet Napolitano warned of an "imminent cyber 9/11."[4] Some in the entertainment industry have even likened the cyber attacks on Sony with the attacks of September 11, 2001 (see Figure 1). While this comparison is an exaggeration of both

the importance of the entertainment industry and the scale of the attack, the Sony attacks exposed the average American to a threat of which they were likely unaware.

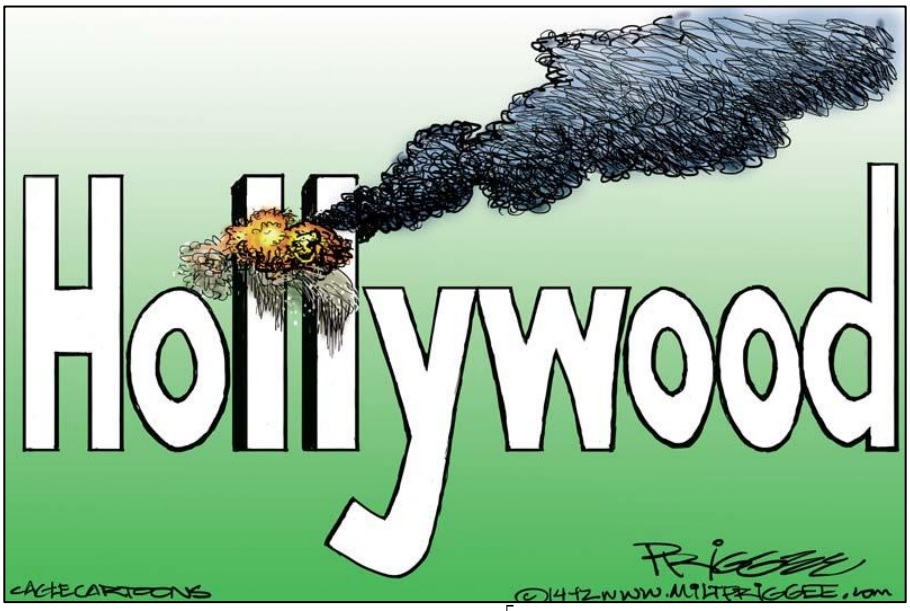

Figure 1[5]

Scholars have not defined this war either. They have raised the issue. John Stone's 2012 article, "Cyber War *Will* Take Place!" argues that cyber war *could* take place but he spends much of his energy attempting to define war. In the end, Stone offers no definition of war, let alone cyber war.[6] Gary McGraw, in his article "Cyber War is Inevitable (Unless We Build Security In)" argues that the considerable hype surrounding cyber war is warranted. His attempt to define cyber war culminates with the assertion that, the "means may be virtual but the impact should be physical." McGraw's idea of cyber attacks impacting the physical world bridges the gap between those who believe in a nonviolent cyber war and those who do not.[7]

Contrasting opinions are offered by theorists who do not believe in the stand-alone cyber war as described by their contemporaries. The key point to emerge in the debate about cyber war is the question most germane to this study: Can cyber war stand on its own? If so, is this a good thing? Erik Gartzke refers to the notion of imminent total cyber war as "cyber pessimism" and

notes that advocates of cyber war focus on the capabilities over the consequences. But Gartzke fails to explain how tasks commonly associated with military violence will be accomplished in the cyber domain.[8] Thomas Rid, in his 2013 book *Cyber War Will Not Take Place*, takes this idea one step further by characterizing the use of the cyber domain in conflict as equivalent to espionage or sabotage.[9] These ideas are echoed in his article, "More Attacks, Less Violence," which was written as a response to criticism from John Stone in, "Cyber War *Will* Take Place!"[10]

Current military doctrine dismisses the idea of a war contained solely within cyberspace. Army Doctrinal Publication 1 (ADP-1) defines cyberspace as a "technical repository and means of transit for information, but its content originates with people on land." ADP-1 goes on to say, "inserting ground troops is the most tangible and durable measure of America's commitment to defend American interests. It signals the Nation's intent to protect friends and deny aggression."[11] Joint Publication (JP) 3-12, "Cyberspace Operations" states, "While it is possible that some military objectives can be achieved by [Cyberspace Operations] alone, [Cyberspace Operations] capabilities should be considered during joint operation planning, integrated into the [Joint Force Commander]'s plan, and synchronized with other operations during execution." JP 3-12 describes cyberspace as one of the five "interdependent domains" and states that "cyberspace effects are created through the integration of cyberspace capabilities with air, land, maritime, and space capabilities."[12] Doctrinally, the Department of Defense appears to be leaning towards the use of cyber integrated with other domains.

Any study of the nature and character of warfare is incomplete without reference to either Clausewitz or Sun Tzu. Mr. Michael Warner, Command Historian of United States Cyber Command, relies heavily on the writings on Sun Tzu to describe cyber warfare.[13] Specifically, he focuses on the four ways of beating an opponent as described by Sun Tzu in Chapter 3 of *The*

Art of War. Other theorists (including Rid and Stone) refer to Clausewitz to determine their definitions of cyber warfare. They debate with how the relationship between force and violence in the Clausewitzian definition of war applies to cyber war.[14] Considering cyber theorists of today refer to the writings of both Sun Tzu and Clausewitz, the ideas of *The Art of War* and *On War* have stood the test of time, even when they are extended into the domains of air and space.[15] It is much too early to say definitively whether the cyber domain would change warfare so drastically as to alter these seemingly timeless definitions.

In order to determine whether a standalone cyber war is possible, one must first define the term. Breaking down the term into the two nouns, cyber and war, provides little assistance in developing us with a definition. No universal definition of war exists. Scholars often point to Clausewitz' definition of war as "an act of force to compel our enemy to do our will."[16] He goes on to say, "War is a continuation of policy by other means."[17] Interestingly, neither of these excerpts from Clausewitz rules out cyber warfare as a possibility; as long as operations within the cyber domain are used as an extension policy, by Clausewitz' definition they could be considered warfare. The same holds true for economic warfare and information warfare, albeit cyber warfare is likely a subset of the latter. Although written long before the Information Age, the ideas in *On War* are timeless and could encompass the idea of cyber warfare.

The Marine Corps expands upon the Clausewitz definition and narrows focus on the military actions during war. Two specific methods of imposing will on the enemy are discussed in the primary reference Marine Corps Doctrinal Publication 1, *Warfighting*: physical destruction of enemy military capabilities and erosion of the enemy leadership's will.[18] Both methods, in theory, are possible through the cyber domain; although the will of the enemy leadership is likely more susceptible to cyber attack than are his military capabilities.

George Santayana once said, “Those who cannot remember the past are condemned to repeat it.”[19] Much of what has been written about theories of cyber warfare strike a similar tone to early twentieth century writings about the future of air warfare. The Italian airpower theorist Giulio Douhet, in his thesis *Command of the Air*, proclaimed the decisiveness of aircraft and their superiority in battle to destroy the will of the people over all other forms of warfare. “The decisive field of action will be the aerial field,” he wrote. It was once believed that the airplane would revolutionize the character of war.[20]

Modern theorists are falling into the same trap, describing cyber warfare as the decisive form of bloodless battle. In many estimations, cyber is a truly revolutionary method by which an adversary can win the fight without fighting, in true Sun Tzu fashion. But as Robert Pape points out in his article, “The True Worth of Air Power,” a major problem with relying solely on aircraft is the lack of ground forces to stabilize a country when it is most vulnerable.[21] This lends credence to the Marine Corps Doctrine of combined arms warfare, the Marine Air Ground Task Force. Cyber, in the future, will fall into the realm of combined arms warfare as another capability available to the commander.[22] Only through the use of combined arms, including cyber, can the will of the enemy be broken. A comparison to the historic debate over airpower and the current discussion of cyber warfare will give this point greater refinement, emphasis, and clarity.

Early Theories of Air Power

Two years after the founding of United States Cyber Command, the United States Department of Defense in 2011 identified cyberspace as a “new domain of warfare." A historic parallel exists with the addition of the air domain in the early 20th century. From the founding of the United States Air Force until today, American policymakers have attempted to accomplish

strategic objectives using military aviation assets only. Following this historical example, it is likely that future policy makers will attempt to wage a war contained solely within cyberspace.

In 1943, scholar Edward Warner wrote, "the airplane possesses such ubiquity, and such advantages of speed and elevation, as to possess the power of destroying all surface installations and instruments, ashore or afloat, while remaining comparatively safe from any effective reprisal from the ground."[23] Warner reflected the reverence Americans held for aviation during the bulk of the 20th century and today, that conflicts can be resolved, or the enemy's determination can be broken, by the use of air power alone.[24] This is not a universally accepted concept, as noted by the Army Doctrinal Publication 1 that states firmly, "No major conflict has ever been won without boots on the ground. Strategic change rarely stems from a single, rapid strike, and swift and victorious campaigns have been the exception in history."[25]

General William "Billy" Mitchell was an early aviation theorist, and controversial figure, still studied today. He is credited with predicting the Japanese surprise attack on Pearl Harbor eighteen years before its occurrence. He also believed that the power of aircraft and rockets to enable travel over long distances would reduce or nullify the geographical protection the United States enjoyed. General Mitchell's predictions for long-range aerial attack have been proven through the use of cruise missiles in recent conflicts; and he also forecast the existence and military use of unmanned aerial vehicles.[26] The military does use aircraft for a myriad of reasons, many of which are included in General Mitchell's theories.

The Italian airpower theorist Guilio Douhet once said, "Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after changes occur." Douhet and Mitchell both believed that the source of the enemy's power, or his center of gravity, was the will of the people. Destroying the enemy's industry and targeting

civilian population would bring a quick, decisive victory. This was not an entirely new concept, as only five years before Douhet was born, William T. Sherman conducted his "march to the sea" with the intent of breaking the will of the Confederacy.[27] Douhet believed that aircraft would fundamentally change the way countries waged future wars. While Sherman's march took a little over a month and required considerable manpower, the dawn of aviation could bring about the same effect more quickly and without the substantial risk to life. The possibilities of cyber warfare are often viewed in this same light today.

During World War II, both British and American air forces followed the theory of the day and attempted to gain decisive advantages using massive aerial attacks. The United States and United Kingdom conducted massive bombing campaigns against German strategic targets and population centers. The goal was to bring a nation to terms via the air alone. As stated by Douhet: "No longer can areas exist in which life can be lived in safety and tranquillity [sic], nor can the battlefield any longer be limited to actual combatants. On the contrary, the battlefield will be limited only by the boundaries of the nations at war, and all of their citizens will become combatants, since all of them will be exposed to the aerial offenses of the enemy."[28] The target was the will of the people, much as it was during Sherman's march to the sea; although, Sherman's land assault was successful, the air assaults on Germany were not.

On the Pacific Front, Major General Curtis E. LeMay and Lieutenant Colonel Robert McNamara led the United States in a massive firebombing campaign in accord with Douhet's writings: to destroy the enemy's center of gravity, the will of the people.[29] Not only did these bombing campaigns fail to decisively end the war, but also the means by which LeMay was attempting to reach the political goal were disproportionate. Clausewitz warned, "the political object is the goal, war is the means of reaching it, and means can never be considered in isolation

from their purpose."[30] The Germans and Japanese endured countless attacks on infrastructure and population. Attacks so intense that scholars to this day still debate whether they were necessary, moral, or even a war crime.[31] Robert McNamara admits that had the Allies lost the war, they would have been prosecuted as war criminals.[32] The massive bombing campaigns of World War II were possible only because the rules of war had not yet been established. The evolution of cyber warfare is in a similar position now. There is no international treaty on the conduct of cyber warfare, no "road map for international response."[33]

In recent years, US leaders continue to argue the overwhelming capabilities of aviation warfare. The promise is swift victory by achieving air superiority through destruction or otherwise mitigation of the enemy's air defense system before targeting the head of state (or the highest profile target). Examples where the U.S. military leadership planned for a quick resolution to military action through the use of airpower include operations during the Persian Gulf War in 1991, Kosovo in 1999, and again during Operation Iraqi Freedom in 2003. These air campaigns were successful in achieving air superiority. The same effect *could* theoretically be achieved using in the cyber domain, but in practice would require an unachievable amount of research and development as well as an unrealistically cooperative target. Precision air strikes designed to kill Saddam Hussein were altogether a failure.[34] U.S. airstrikes intended to persuade President Milosevic into changing his policies failed and ultimately backfired when the Serbian military killed thousands and expelled nearly a million people from the country.[35] Thus, while US forces were successful in achieving air superiority, the follow-on targeting of heads of state failed to capitalize on the successes in the air.

A major problem with this strategy of using air assets to "decapitate the enemy," as Robert Pape calls it in his article in *Foreign Affairs,* is the lack of ground forces to stabilize the

country when it is most vulnerable after the strikes have been successful.[36] Relying solely on aviation assets contributes to the void created by the elimination of leadership. The United States military is truly effective when aviation acts as a supporting asset to the troops on the ground. The same holds true for cyber. Suppose a cyber attacker could target and kill a leader. Ground forces would be required to stabilize the region and help guide the country to rebuild a new government. In order to ensure success in the future, cyber operations must be incorporated into the combined arms concept.

Douhet and his contemporaries, the airpower theorists of the early 20th century, believed the advent of the airplane revolutionized the character of war. Instead, the airplane was simply another tool for the military commander to use in the attempt to defeat the enemy. The airplane has fallen into the same category as the tank, artillery, rifle, and naval warship. All are conventional kinetic methods by which one commander can attack and attempt to break an enemy's resolve. Even at the time of his writings, Douhet's ideas were met with criticism. He addressed several of his critics by paraphrasing their arguments as, "The aerial field is decisive – when it is decisive." This, he claimed, was consistent with his assertions and he continued to assert that his critics actually agreed with him. Yet, as one expert observed, "Much that he predicted, of course, turned out to be incorrect." This includes his assessments of the destructive capability of a ton of bombs as well as the capabilities attacking aircraft against a defense.[37]

Advocates in the early 20th century considered the aircraft, particularly the bomber, invincible. Douhet saw no effective measure that could defend against an enemy determined to bomb cities.[38] Like many new technologies, though, the advantage was enjoyed for only a short time until a counter weapon was developed. Germany began perfecting the technology of ballistic anti-aircraft artillery during the Second World War.[39] The Nike Ajax, the first US

surface-to-air missile (SAM) system, was tested successfully in 1951.[40] Soon, nations developed integrated air defense systems by combining anti-aircraft artillery, fighter aircraft, and SAM systems to defend against airborne attack. For each new aircraft built, a new countermeasure appears as soon as adversarial countries understand the new technology and can afford to research and develop a method to combat it.

The cyber threat mirrors the aviation domain in this respect and with a vengeance since the technology is relatively cheap and widely available.[41] Defense networks can be established with features that are concealed to the attacker such as firewalls and honeypots. A cyber form of a decoy, these honeypots can be built so the cyber attacker is not aware he is not striking the actual targeted system. While the attacker explores the honeypot, the victim can monitor the attacker's every move.[42] If victims of cyber attacks can determine where the attack originated, which can be nearly impossible if the attacker is skilled enough, they have an extensive range of options. An active response would be to conduct retaliatory attacks or "hack-backs" aimed at the attacker's servers. Once access is obtained, the hack-back could consist of finding and deleting stolen information or infecting the network with a virus, or anything in between.[43] More passive forms of response include identifying the attacker's internet protocol (IP) address and blocking the IP address from accessing the server. There are many options available to the cyber security professional. The differences between defense in the cyber domain and the air domain include the accessibility, affordability, and rapid evolution of defensive cyber measures. Both state and non-state actors alike easily operate within the cyber domain, which can level the playing field between conventionally asymmetric forces in a way air power could not.

The Cyber Domain

The five most commonly acknowledged domains of warfare are land, sea, air, space, and now cyber.[44] Land and sea warfare both have been in existence for centuries and are complementary to one another. The advent of aviation warfare, as discussed here, led many to believe that the land and sea domains were outdated. However, despite the fact that swift victory through air attacks is still attempted, history has shown that the key to success is domination in all three domains, particularly air and land. The space domain is relied upon primarily for global positioning systems and satellite technology, including imagery.[45] Space weapons are largely a thing of the future and science fiction;[46] however, the Committee on the Peaceful Uses of Outer Space has maintained five treaties governing the use of the space domain since 1966.[47] In contrast, the only treaty that currently governs cyberspace is the Council of Europe Convention on Cybercrime, which deals largely with criminal activity such as copyright, fraud, child pornography, and violations of network security.[48] Currently, the Geneva Conventions do not address cyber warfare directly; however, international humanitarian law would apply should a belligerent use cyber operations in conjunction with traditional armed warfare.[49]

The first theorists developed the idea of a worldwide network of connected computers in the early 1960s. Within two decades, the Department of Defense began requiring all new computer purchases to be internet-capable.[50] One of the primary keys to the successful development of what we today refer to as "the internet" is the idea of open-architecture networking. There would be no requirements for existing networks to change in order to connect to the Internet, and there would be "no global control at the operations level."[51] This basic premise of the Internet allows for freedom of maneuver, making the cyber domain most similar to the sea domain.[52] The primary difference between the two domains is the global reach of

cyber networking. Just as the air domain is used primarily to support both the land and sea domains, cyber can support operations in all five domains.

The history of the use of the cyber domain in conflicts is short, beginning in the early 1980s. In 1981, the contents of the *Farewell Dossier* provided U.S. intelligence with inside knowledge on the Soviet intentions to modernize their infrastructure. The plan, referred to as the "Weiss Project" by Thomas C. Reed, was to provide Canada with software to sell to the Soviets. This software, enhanced by the U.S. Central Intelligence Agency (CIA) would be used by the Soviets for an assortment of infrastructure requirements, particularly the Trans-Siberian Pipeline. Thomas C. Reed alleges that the computer chips and software would pass initial operational testing but, once installed and in use, intentional errors in the software, or trojan horses, planted by the CIA would cause the system to malfunction, the result being "the most incredible non-nuclear explosion and fire ever seen from space."[53]

The trouble with cyber attacks is that it is easy to incorrectly categorize the incident. The Trans-Siberian Pipeline incident is widely disputed as to whether it was a result of malicious code in the software or other faulty equipment. Assuming, for argument's sake, that it happened exactly as Thomas Reed described it to be, a logic bomb. [54] Was it an act of war? At the time, the U.S. and Soviet Union were deeply embroiled in the Cold War. If this was a cyber attack on the Soviets by the U.S. with a helping hand lent from Canada, and if the Soviets had realized it at the time, would that have been enough to force the Soviets to wage a counterattack? If the Soviets had chosen to launch a counterattack, would they have used cyber or kinetic means? These are all questions strategists now must consider. Given the situation as accounted by Thomas Reed, I conclude that the cyber attack on the Trans-Siberian Pipeline was cyber sabotage by logic bomb in order to destroy the pipeline for US political advantage during the

Cold War.[55] More importantly, though, due to the nature of the "attack" and the continued disagreement regarding the facts surrounding the incident, it is not possible for this example to have been a decisive act of war due to the fact that the aggressor, if it exists, is unknown.[56]

More examples of the military use of cyberspace have occurred in the last decade. In 2007, Israel launched a combined cyber-kinetic attack on Syria.[57] The details of Operation Orchard, as it was called, are still classified but it is likely that Israel used computer coding to sabotage the Syrian air defense network, rendering it incapable of detecting the squadron of Israeli F-15s and F-16s that entered the country, bombed the nuclear facility, and then departed the airspace. Once neutralized, the air defense network had to appear as though it was still operating properly or risk providing an indication to the Syrians of the malfunction.[58] This form of combined-arms attack using both cyber sabotage and traditional military forces is likely to be the way of the future – and is in keeping with the evolution of the use of aircraft in combat. In contrast to the air power theorists and military leadership, aviation has proved most effective in a supporting rather than a solitary role.

Another cyber attack in 2007 occurred when Russia responded to growing tensions by launching a distributed denial of service (DDoS) attack on Estonia. The attack began with a less-sophisticated denial of service (DoS) attack. As the perpetrators worked to make the attack more complex, botnets were used to coordinate the attacks and increase the volume, leading to the DDoS attacks. Up to 85,000 computers were hijacked, and Estonia felt the effects of the attacks for three weeks. Most of the effects were minor, but because targets included the country's banking system the attacks alarmed the Estonian leadership.[59] NATO did not classify the DDoS attacks on Estonia as an event worthy of military response. Further, the Council of Europe Convention on Cybercrime determined that a criminal investigation by Interpol would have been

the proper response. The Assistant Director of the U.S. Federal Bureau of Investigation's Cyber Division agreed.[60] These two authorities confirmed that these DDoS attacks were cybercrime, not decisive acts of war.

Prior to the recent North Korean cyber attack on U.S. entertainment company Sony, one of the most widely known cyber attacks, known as Stuxnet, targeted a nuclear enrichment facility in Iran. The idea was to insert thousands of lines of code into the computer system that operated the high-speed centrifuges to cause faults within the valves and alter the pressure within the centrifuge. To the facility personnel, the reasons for the failure could be unlimited to include human error or defective equipment. The alleged political goal was for the U.S., with the help of Israel, to degrade Iran's ability to build a nuclear weapon by preventing them from turning gaseous uranium into weapons-grade material.[61]

One of the challenges that the designers of Stuxnet faced – an obstacle that is not unique to their endeavor – was that the centrifuge computers they wished to infect with their code were part of a closed network.[62] This meant that the code could not be sent remotely, but rather had to be uploaded by someone or something inside the facility. Here, the cyber attack crosses path with traditional methods of sabotage and espionage. The initial attacks, under President George W. Bush, were implemented and effective. Upon assuming office, President Barack Obama focused on denying Iran's ability to build nuclear weapons and ordered the code be altered to damage the equipment by causing the centrifuges to spin at dangerously high speeds.[63]

Ultimately, a security company in Belarus discovered the virus.[64] How Stuxnet got to Belarus when originally installed within a closed network is part of the design of the virus. Not only was it designed to sabotage the Iranian nuclear facility, but it was also designed as a form of espionage. If any personnel plugged in a laptop to the facility's network, Stuxnet would transfer

to the laptop and then transfer to any other network to which the laptop was subsequently connected. The virus was also a form of espionage by which the U.S. could potentially identify other nuclear processing facilities within Iran, and then infect those centrifuges as well.[65]

The Pentagon, in 2011, determined that computer sabotage launched by a foreign country would be considered an act of war to be met with a response of traditional military force.[66] In the Trans-Siberian Pipeline example, the Soviets may have been unaware that they were victim to an act of cyber sabotage and, if they suspected, they may not have been able to accurately trace the origins back to the United States. Herein lie the difficulties of responding to a cyber attack: First, am I aware of the breach and, second, can I figure out who is responsible? As offensive cyber technology grows more advanced, these questions are getting more difficult to answer. With the widespread availability of inexpensive and advanced hacking software, a government may be able to determine the source of the attack only to find a non-state actor operating within the borders of a friendly country. This further complicates the issue.

Espionage, as described by the Spy Museum in Washington D.C., is the second-oldest occupation.[67] It is a concept that is dates back to the earliest origins of human history; Sun Tzu discussed deception and subversion in *The Art of War*.[68] The methods by which people have conducted espionage have changed through time as technology has advanced. The use of computer networks and the cyber domain is a natural path for the activity of espionage to follow. Much of the cyber activity between nations could be classified as cyber espionage.

Nations do not limit their use of espionage only to times of war. Nations and non-state actors are constantly interested in the inner-workings of both friend and foe, and one of the best ways to gain intelligence is through espionage. The cyber domain has made espionage less risky to countries who can stage their operatives anywhere and cover their tracks through elaborate

programs so that, if discovered, the origins of their operation are difficult to determine.[69] Espionage is inherently non-kinetic, where the purpose is to gain information about plans or activities of another government or competing company.[70]

The historical examples of the use of cyberspace in conflict as mentioned here generally fall into one of three categories: cyber espionage, cyber sabotage, or combined cyber-kinetic warfare. History has not supplied a precedent for the response to any form of cyber attack;[71] the attacks have usually been short and the attackers have apparently gotten away with them. The U.S. has already stated the intention to treat cyber sabotage as an act of war, but the definition of cyber sabotage is largely unclear.[72] In 2012, many American banks came under DDoS attack from a group self-identified as Izz ad-Din al-Qassam Brigades. In his book *@ War*, Shane Harris speculates that the attacks may have been retribution for the Stuxnet virus. Is a DDoS attack on the banking system, which does no real harm beyond causing panic among bank security personnel, worthy of a military response? What is the threshold for military response? Finally, if the political leadership determined military response was warranted, would that response remain contained to cyberspace?

Based on the known incidents since 2007, kinetic responses to acts of cyber sabotage seem unlikely. However, whether cyber sabotage and cyber espionage count as cyber war is yet to be determined. If Clausewitz' description of war holds true, cyber warfare is not war because it lacks violence and it lacks force.[73] In some cases, perpetrators of cyber attacks have no political goal, which renders their actions more in line with cyber crime than cyber warfare for without a political goal these attacks cannot be "a mere continuation of policy by other means."[74] Ultimately, though, cyber attacks lack the capability to break one country's will and bend it to another. Using cyberspace, nations and non-state actors alike can harass, deceive, and subvert

one another effectively; but if the victim's existence is truly threatened, the response will not be through cyberspace. The response will be kinetic and involve actions within each of the five domains of warfare to ensure a swift victory.

Recommendations

The Marine Corps should look to the history of the integration of aviation into the service for a historical road map that suggests how to integrate cyber into the Corps. Perhaps one day, instead of doctrinally working as a Marine Air Ground Task Force (MAGTF), the Marine Corps will be organized into Marine Cyber Air Ground Task Forces (MCAGTF). The failure to incorporate cyber fully into the Marine Corps and ensure that all Marines are considering offensive but, more importantly, defensive cyber operations, will forfeit the nation's technological superiority and set Marines up for failure against technologically advanced adversaries. This will lead to the type of fight we seek to avoid: protracted, expensive conflicts with high casualty rates. The Marine Corps is America's force in readiness and that should include capabilities to wage a combined arms assault across all domains.

One of the lessons easily learned from the Corps' experience with aviation combat element that should be implemented is how Marines are assigned military occupational specialties (MOSs) as pilots, naval flight officers (NFOs), or unmanned aerial system (UAS) officers. Marine Officers currently interested in those three MOSs must pass the Aviation Selection Test Battery (ASTB), which is a test encompassing skills and talents required of an aviator. The test is scored in three areas, with one as the lowest score and nine as the highest for each area. The highest grade possible, for example, is a 9/9/9.[75] Upon earning a qualifying grade on the ASTB and passing requisite physical requirements, Marine officers are eligible to contract as a pilot or NFO contract. This contract incurs additional time in service upon

completion of flight school.

What I am proposing is not only that the Marine Corps create a cyber MOS – I think that is an obvious next step for any service and the Air Force and Army have already created cyber MOSs.[76] In addition to recruiting at schools where cyber-related degrees are awarded, the DoD should create a cyber test (similar to the ASTB) to screen potential candidates for cyber capabilities. The test could include questions on common code languages, like C++, or it could be arranged similar to the Defense Language Aptitude Battery (DLAB). The DLAB tests a candidate's aptitude for learning a foreign language based on her ability to remember language rules and decipher phrases of a pretend language.[*] The difference would be testing for aptitude to learn programming skills versus actual programming skills, the former likely being easier to recruit than the latter. Once candidates earn the requisite score on the cyber test, they would be eligible for a military cyber contract.

The reason for an additional form of contract is two-fold: to insure that eligible Marines are guaranteed the cyber MOS and to increase retention within the MOS. Major General Donahue, commanding officer of Marine Forces Cyber Command (MARFORCYBER), recognizes the challenge of retaining cyber Marines because the civilian sector offers higher pay for cyber skills than the military. Another way to combat this attrition, in addition to the extended contracts, would be to provide incentive pay to cyber Marines. This would help bridge the wage gap between the DoD and civilian sector in much the same way that flight pay does for aviators while ensuring the cyber warriors are trained in Marine Corps operations as part of a combined arms fight. How to attract the, "best and brightest" to military service is on the minds of senior leadership, including Defense Secretary Ash Carter.[77] A successful example exists in

[*] Author took the DLAB in October 2013.

the recruitment and retention of aviators, a historical lesson waiting to be applied to the current problem.

As a result of the fast-paced, ever-changing nature of cyber technologies, the career path of a cyber Marine should also be slightly different from the average Marine. A typical Marine, once complete with MOS school, proceeds to the operating forces for a tour of three years. Upon completion of the first tour, Marines normally transition to a "B Billet," or another position in the Marine Corps outside of their assigned MOS. After a three year "B Billet," Marines then return to their MOS for another tour.

A cyber Marine who follows this traditional career path, would require extensive refresher training upon returning to the operating force after the "B Billet" due to not only deterioration of skills but also the rapidly changing nature of the technologies and threats. My proposal is to have operational tours for cyber Marines within MARFORCYBER and US CYBERCOM. These could be billets physically located with the command or billets on teams that are assigned to geographical combatant commanders or MAGTF commanders worldwide. "B Billet" options for cyber Marines could be liaison billets with the Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency, Department of Homeland Security, joint services, etc. These "B Billets" would afford the opportunity for the Marines to get out of the operating forces and become well-rounded Marines while maintaining their cyber skills. The implementation of cyber warriors should follow the lead of the implementation of air warriors using testing, contracting, and incentive pay as a reference.

Beyond the recruitment and retention of cyber warriors, every Marine needs to be trained to consider the use of the cyber domain as part of Marine Corps combined arms doctrine. Each service offers professional military education opportunities to improve the quality and training of

its personnel. Which school service members attend depends on their service and pay grade. The primary Marine Corps enlisted schools are Corporals Course, Sergeants Course, Career Course, Advanced Course, Staff Non-Commissioned Officer (SNCO) Academy, and a myriad of other Senior Enlisted Courses.[78] All Marine Officers initially begin their time in service with six months of leadership training at The Basic School. Then, in order to be promoted through the ranks, Marine Officers must attend, or complete by way of distance education: Expeditionary Warfare School, Command and Staff College, and the War College.[79]

While each of these schools has a different focus, the schools geared toward officers and SNCOs include formal instruction on as well as hands-on practical application exercises of the Marine Corps Planning Process (MCPP) as appropriate to the pay grade and level of warfare (tactical, operational, or strategic).[80] These courses should include, at a minimum, an overview of cyber operations in order to expose all students to this new domain of warfare and considerations for use of cyber as part of combined arms operations. This can be accomplished in an unclassified forum with historical examples of uses of cyber such as the aforementioned DDoS attacks on Estonia and the integrated cyber-kinetic Israeli attack on Syria.

As the services become increasingly reliant on networked connectivity, service members, particularly those in leadership positions, need to be aware of the dangers that they may face. Command and Staff College currently includes a one-hour cyber introduction lecture and offers two optional courses, one classified and one unclassified, that students can opt to take as electives. The one-hour introductory lecture fails to illuminate the significance of cyber to the warfighter. The small class sizes of the optional electives limit the exposure of cyber warfare to the student body, and those who sign up for the class generally have some prior knowledge of the topic. The curricula for the SNCO and officer PME courses should fully incorporate cyber

warfare operations because all leaders will need to consider cyber operations within their planning of combined arms operations; failure to do so forfeits the capabilities within an entire domain to a technologically advanced future adversary while Marine leaders prepare to fight the conflicts of yesterday.

To fully prepare Marines for the conflicts of tomorrow, the scenarios used for exercises both at PME schools and in the operational forces should include a cyber component. The hands-on planning exercises at the PME schools are currently missing an opportunity to teach planners to include the cyber resources in their threat assessment and planning. It may be a challenge to keep the cyber threat discussion unclassified (as many of the planning exercises are not classified) but the planners of the future need to be considering the cyber threat. The enemy role players, the "red cell," and the civilian or non-governmental operations role players, or "green cell," should also include cyber in their planning and execution.[81] Most importantly, scenarios should be designed to be as realistic as possible in order to challenge both planners and executors of the mission.

Realism in the training scenarios provides effective training to the service members. Failure to realistically represent the situation, or "fairy dusting" as we often call it, occurs too often when training environments are simplified to make them more manageable. This phenomenon should be limited to the maximum extent possible. Neither fairy dusting the situation nor painting a challenging scenario presented by the red cell as impossible sets up planners and their troops for success. In the introduction of his book, *7 Deadly Scenarios,* author Andrew F. Krepinevich discusses this very flaw in military training scenarios. He specifically cites three examples of scenarios, the first of which was the most shocking. It seemed to follow step-by-step the December 7, 1942 Japanese attack on Pearl Harbor. Instead, it was a

recollection of a February 7, 1932 war game during which U.S. Rear Admiral Harry Yarnell, acting as the red cell commander, seemingly predicted the actions Japanese Admiral Yamamoto would take nearly ten years later. The Army Air Corps denied the effectiveness of the red cell's attack, poking holes at the alleged levels of damage to Hickam Field and claiming that they had found the red cell aircraft carriers. The most striking of all the fairy dusting was the Army Air Corps' protest that, "it was improper to begin a war on a Sunday!"[82] In my experience in PME, I believe we have not yet learned from these mistakes. Realism is lacking in our scenarios, and the friendlies always win. While this boosts our confidence – and confidence in battle is necessary to the warfighter – overconfidence can prove disastrous. The failure to include cyber operations in exercises detracts from the realism of the scenario and generates Marines who are ignorant to the newest tools available in the combined arms fight of the future.

Conclusion

This paper has analyzed how a new and exciting military capability – the cyber domain of warfare – is being addressed in much the same way as the new military capability of air operations was treated a century ago. The research to support the thesis of this paper has provided some insight as to the future of the integration of cyber operations into the Marine Corps. We should look to history for examples of both fear and sensationalism in the perceived threats posed by first generations of new military capabilities. As addressed here, current theories promoting bloodless cyber warfare will lead us away from the more sound military use of cyber operations as a function of warfare integrated into the traditional kinetic approach.

Nations are approaching cyber warfare differently. This is due primarily to differences in legal structures. The current legal structure of the U.S. forces requires Presidential approval for cyber strikes.[83] While these permissions should also be reviewed, the Marine Corps can work

within the current confines of the law and begin structuring the force to conduct combined arms operations including land, sea, air, space, *and* cyber. Should the current legal definition of cyber attacks change, the Marine Corps will be even more prepared for what may be a more decentralized method of cyber operations. That way, the Marine Corps will be prepared for the battlefield of the future – which is less likely to be the bloodless battlefield limited to cyberspace than a combined arms fight during which cyber operations are used to minimize risk to friendly forces while maximizing impact on the enemy.

Endnotes

[1] Shane Harris, *@ War: The Rise of the Military-Internet Complex* (New York: Harcourt, 2014).
[2] Richard Clark, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012).
[3] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *NYTimes.com*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.
[4] Reuters, "U.S. homeland chiefL cyber 9/11 could happen 'imminently,'" *Reuters.com*, January 24, 2013, http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124.
[5] Priggee, Milt, editorial cartoonist, "Hollywood," cartoon, MiltPriggee.com, National Cartoons Collection, http://www.miltpriggee.com/cartoons/national/view/9407/.
[6] John Stone, "Cyber War *Will* Take Place!" *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013), 101-108.
[7] Gary McGraw, "Cyber War is Inevitable (Unless We Build In Security)," *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013), 112.
[8] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013).
[9] Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 42.
[10] Thomas Rid, "More Attacks, Less Violence," *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).
[11] Headquarters Department of the Army. *The Army.* ADP 1. (Washington, DC: Headquarters Department of the Army, November 7, 2012).
[12] U.S. Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (R) (Washington, DC: Department of Defense, February 5, 2013).
[13] Michael Warner, "US Policy in Cyberspace" (lecture, Marine Corps University, Quantico, VA, January 2015).
[14] Stone, "Cyber War *Will* Take Place!" 106.
[15] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984).
Sun Tzu, *The Art of War*, Samuel B., Griffith, ed. and trans. (New York: Oxford University, 1971).
[16] Clausewitz, *On War*, 75.
[17] Clausewitz, *On War*, 87.
[18] Headquarters U.S. Marine Corps, *Warfighting*, MCDP 1, (Washington, DC: U.S. Marine Corps, June 30, 1991), 24-25.
[19] George Santayana, *The Life of Reason*, vol. 1 (New York: Dover Publications, 1980), http://www.gutenberg.org/files/15000/15000-h/vol1.html.
[20] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (Washington, DC: Air Force History and Museums Program, 1998), 9-10, http://www.au.af.mil/au/awc/awcgate/readings/command_of_the_air.pdf.
[21] Robert A. Pape, "The True Worth of Air Power," *Foreign Affairs*. March/April 2004, Accessed December 13, 2014, http://www.foreignaffairs.com/articles/59714/robert-a-pape/the-true-worth-of-air-power.
[22] U.S. Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (R) (Washington, DC: Department of Defense, February 5, 2013).

[23] Edward Warner, "Douhet, Mitchell, Seversky: Theories of Air Warfare," in *Makers of Modern Strategy: From Machiavelli to Hitler*, 485.
[24] Eliot A. Cohen, "The Mystique of U.S. Air Power," *Foreign Affairs*, January/February 1994. Accessed February 25, 2015, http://www.foreignaffairs.com/articles/49442/eliot-a-cohen/the-mystique-of-us-air-power.
[25] Headquarters Department of the Army, *The Army*, ADP 1 (Washington, DC: Headquarters Department of the Army, November 7, 2012).
[26] Douglas Waller, *A Question of Loyalty*, 5-6.
[27] "Sherman's March," *History.com*, Section "March to the Sea," accessed February 19, 2015, http://www.history.com/topics/american-civil-war/shermans-march.
[28] Douhet, *The Command of the Air*, 9-10.
[29] Douhet, *The Command of the Air*, 9-10.
[30] Clausewitz, *On War*, 87.
[31] Public Broadcasting Station, "People & Events: General Curtis E. LeMay, (1906-1990)," PBS.org, accessed March 30, 2015, http://www.pbs.org/wgbh/amex/bomb/peopleevents/pandeAMEX61.html.
[32] "McNamara Bombing Japan," (Excerpt from the 2003 Documentary *Fog of War*), video, 06:01, posted by VilhelmAxel, https://www.youtube.com/watch?v=cdmfPThGZ-s.
[33] Harris, *@ War*, 51.
[34] Cohen, "The Mystique of U.S. Air Power."
[35] Pape, "The True Worth of Air Power."
[36] Pape, "The True Worth of Air Power."
[37] Douhet, *The Command of the Air*, ix.
[38] Douhet, *The Command of the Air*, 10.
[39] Kenneth P. Werrell, *Archie to SAM : A Short Operational History of Ground-based Air Defense* (Maxwell Air Force Base, Ala: Air University Press, 2005), *eBook Collection (EBSCOhost)*, EBSCO*host* (accessed March 30, 2015), 24.
[40] Werrell, *Archie to SAM*, 83.
[41] "Frequently Asked Questions," Hacker School, last modified February 16, 2015, https://www.hackerschool.com/faq.
[42] Harris, *@ War*, 58.
[43] Harris, *@ War*, 106.
[44] Lynn III, William J., "Defending a New Domain," *Foreign Affairs*, Sept/Oct 2010, Vol. 89 Issue 5, 101.
[45] Cohen, "The Mystique of U.S. Air Power."
[46] "Top 10 Space Weapons," Space.com Staff, last modified April 5, 2013, http://www.space.com/19-top-10-space-weapons.html.
[47] "United Nations Treaties and Principles on Space Law," United Nations Office for Outer Space Affairs, last modified December 4, 2014, http://www.unoosa.org/oosa/en/SpaceLaw/treaties.html.
[48] "Convention on Cybercrime," Council of Europe, last modified November 18, 2014, http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.
[49] "The Law of War Imposes Limits on Cyber Attacks, Too," International Committee of the Red Cross, last modified October 14, 2013, https://www.icrc.org/eng/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm.
[50] "Brief History of the Internet," Barry M. Leiner et al, Internet Society, Section "Commercialization of the Technology," http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.
[51] "Brief History of the Internet," Barry M. Leiner et al, Internet Society, Section "Initial Internetting Concepts," http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.
[52] Headquarters U.S. Marine Corps, *Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore*, MCCP 1 (Washington, DC: Headquarters U.S. Marine Corps, January 4, 1996), 16.
[53] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York, NY: Ballantine Books, 2007), Kindle edition.
[54] Reed, *At the Abyss*, Kindle edition.
[55] Paul Lewis, "U.S. Asks Its Allies to Deny to Soviet Parts for Pipeline," *NYTimes.com*, January 11, 1982, http://www.nytimes.com/1982/01/11/world/us-asks-its-allies-to-deny-to-soviet-parts-for-pipeline.html.
[56] Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: Department of Defense, January 15, 2015), 61.

[57] Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 1-3.
[58] Rid, *Cyber War Will Not Take Place*, 42.
[59] Korns, Stephen W. and Kastenberg, Joshua E., "Georgia's Cyber Left Hook," *Parameters* (Winter 2008-2009): 63.
[60] Korns and Kastenberg, "Georgia's Cyber Left Hook," 65.
[61] Harris, *@ War*, 11.
[62] Harris, *@ War*, 11.
[63] Harris, *@ War*, 46.
[64] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013): 365. http://dx.doi.org/10.1080/09636412.2013.816122.
[65] Harris, *@ War*, 46.
[66] Gorman, Siobhan and Julian E. Barnes, "Cyber Combat: Act of War," *WSJ.com*, May 31, 2011, http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.
[67] International Spy Museum, "Searchable Master Script," (written explanation of all material in the museum), last modified August 11, 2013: 68, http://www.spymuseum.org/files/resources/master-script_8_13_13.pdf.
[68] Sun Tzu, *The Art of War*, Samuel B., Griffith, ed. and trans. (New York: Oxford University, 1971).
[69] Harris, *@ War*, 103-111.
[70] Merriam-Webster Online Dictionary, s.v. "espionage," http://www.merriam-webster.com/dictionary/espionage, accessed January 9, 2015.
[71] Harris, Shane. *@ War: The Rise of the Military-Internet Complex*, New York: Harcourt, 2014, 51.
[72] Gorman, "Cyber Combat: Act of War," *WSJ.com*, May 31, 2011, http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.
[73] Clausewitz, *On War*, 75.
[74] Clausewitz, *On War*, 87.
[75] "ASTB-E Overview," Navy Medicine Operational Training Center, last modified July 5, 2013, http://www.med.navy.mil/sites/nmotc/nami/Pages/ASTBOverview.aspx.
[76] "Careers," U.S. Air Force, last modified December 20, 2014, http://www.airforce.com/careers/detail/cyber-systems-operations/ http://www.army.mil/article/123328/Cyber_Network_Defender_MOS_now_open_to_NC.
[77] Lolita C. Baldor, "Pentagon chief considers easing of enlistment standards," *AP.org*, March 30, 2015, http://bigstory.ap.org/article/48643bf7477d44fe833286c057bae99a/pentagon-chief-may-ease-military-enlistment-standards.
[78] "Enlisted Professional Military Education," Marine Corps University, accessed February 26, 2015, https://www.mcu.usmc.mil/epme/SitePages/Home.aspx.
[79] "Marine Officer Professional Military Education Requirements," Marine Corps University, accessed February 26, 2015, https://www.mcu.usmc.mil/SACS1/PME/PME%20by%20Grade%20Officer%20110908.pdf.
[80] Headquarters U.S. Marine Corps, *Warfighting*, 29.
[81] Headquarters U.S. Marine Corps, *Marine Corps Planning Process*, MCWP 5-1, (Washington, DC: U.S. Marine Corps, August 24, 2010), 2-6.
[82] Andrew F. Krepinevich, *7 Deadly Scenarios*, New York: Bantam Dell, 2009, 1-3.
[83] Harris, *@ War*, 51.

Works Cited

Clark, Richard. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2012.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013).

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins, 2010.

Clausewitz, Carl von. *On War*. Edited by Michael Howard and Peter Paret. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Cohen, Eliot A., "The Mystique of U.S. Air Power." *Foreign Affairs* (January/February 1994): http://www.foreignaffairs.com/articles/49442/eliot-a-cohen/the-mystique-of-us-air-power. Accessed February 25, 2015.

Department of Defense. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02. Washington, DC: Department of Defense, January 15, 2015.

Douhet, Giulio. *The Command of the Air*. Translated by Dino Ferrari. Washington, DC: Air Force History and Museums Program, 1998). http://www.au.af.mil/au/awc/awcgate/readings/command_of_the_air.pdf.

Harris, Shane. *@ War: The Rise of the Military-Internet Complex*. New York: Harcourt, 2014.

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

Headquarters U.S. Marine Corps. *Marine Corps Planning Process.* MCWP 5-1. Washington, DC: U.S. Marine Corps, August 24, 2010.

Headquarters U.S. Marine Corps. *Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore.* MCCP 1. Washington, DC: Headquarters U.S. Marine Corps, January 4, 1996.

Headquarters U.S. Marine Corps. *Warfighting.* MCDP 1. Washington, DC: U.S. Marine Corps, June 30, 1991.

Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* (Winter 2008-2009): 60-76.

Krepinevich, Andrew F. *7 Deadly Scenarios.* New York: Bantam Dell, 2009.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* Vol. 22, No. 3 (2013): http://dx.doi.org/10.1080/09636412.2013.816122.

Lynn III, William J. “Defending a New Domain.” *Foreign Affairs* Vol. 89 Issue 5 (September/October 2010): 97-108.

Milt Priggee National Cartoons Collection. MiltPriggee.com. http://www.miltpriggee.com/cartoons/national/view/9407/.

Pape, Robert A. "The True Worth of Air Power." Foreign Affairs. March/April 2004. Accessed December 13, 2014. http://www.foreignaffairs.com/articles/59714/robert-a-pape/the-true-worth-of-air-power.

Reed, Thomas C. *At the Abyss: An Insider’s History of the Cold War*. New York, NY: Ballantine Books, 2007. Kindle edition.

Rid, Thomas. *Cyber War Will Not Take Place.* New York: Oxford University Press, 2013.

Rid, Thomas. “More Attacks, Less Violence,” *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).

Santayana, George. *The Life of Reason.* 5 vols. New York, NY: Dover Publications, 1980. http://www.gutenberg.org/files/15000/15000-h/vol1.html.

Stone, John. “Cyber War *Will* Take Place!” *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).

Tzu, Sun. *The Art of War*, Edited by Samuel B., Griffith. Translated by Samuel B., Griffith. New York, NY: Oxford University, 1971.

U.S. Department of Defense. *Cyberspace Operations.* Joint Publication 3-12 (R). Washington, DC: Department of Defense, February 5, 2013.

Warner, Edward. “Douhet, Mitchell, Seversky: Theories of Air Warfare.” In *Makers of Modern Strategy*, edited by Edward Mead Earle, 485-503. Princeton, NJ: Princeton University Press, 1943.

Warner, Michael. “US Policy in Cyberspace.” Lecture presented at Marine Corps University, Quantico, VA, January 2015.

Werrell, Kenneth P. *Archie to SAM : A Short Operational History of Ground-based Air Defense*. Maxwell Air Force Base, Ala: Air University Press, 2005. *eBook Collection (EBSCOhost)*, EBSCO*host* (accessed March 30, 2015).

Bibliography

Betz, David. “Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed,” *The Journal of Strategic Studies*, Vol. 35, No. 5 (October 2012): 689-711.

Clark, Richard. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2012.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International Security*, Vol. 38, No. 2 (Fall 2013).

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins, 2010.

Clausewitz, Carl von. *On War*. Edited by Michael Howard and Peter Paret. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Cohen, Eliot A., "The Mystique of U.S. Air Power." *Foreign Affairs* (January/February 1994): http://www.foreignaffairs.com/articles/49442/eliot-a-cohen/the-mystique-of-us-air-power. Accessed February 25, 2015.

Department of Defense. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02. Washington, DC: Department of Defense, January 15, 2015.

Douhet, Giulio. *The Command of the Air.* Translated by Dino Ferrari. Washington, DC: Air Force History and Museums Program, 1998). http://www.au.af.mil/au/awc/awcgate/readings/command_of_the_air.pdf.

Flynn, Matthew J. “Is There a Cyber War? Review Essay.” *National Cyber Security Institute Journal*, Vol. 1, No. 2 (2014): 5-8. http://ncij.excelsior.edu/article/is-there-a-cyber-war/.

Hachigian, Nina. “China’s Cyber-Strategy.” *Foreign Affairs* (March-April 2001): 118-133. http://lomc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=4127141&site=ehost-live.

Harris, Shane. *@ War: The Rise of the Military-Internet Complex*. New York: Harcourt, 2014.

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

Headquarters U.S. Marine Corps. *Marine Corps Planning Process.* MCWP 5-1. Washington, DC: U.S. Marine Corps, August 24, 2010.

Headquarters U.S. Marine Corps. *Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore.* MCCP 1. Washington, DC: Headquarters U.S. Marine Corps, January 4, 1996.

Headquarters U.S. Marine Corps. *Warfighting.* MCDP 1. Washington, DC: U.S. Marine Corps, June 30, 1991.

Hollis, David M. "Cyber War Case Study, Georgia 2008." *Small Wars Journal.* January 6, 2011. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Junior, Timothy J. "How Probably is Cyber War?: Bringing IR Theory Back in to the Cyber Debate." *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).

Kanwal, Gurmeet. "China's Emerging Cyber War Doctrine." *Journal of Defence Studies*, Vol. 3, No. 3 (July 2009): 14-22.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security*, Vol. 38, No. 2 (Fall 2013): 7-40.

Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* (Winter 2008-2009): 60-76. http://www.carlisle.army.mil/USAWC/parameters/Articles/08winter/korns.pdf.

Krepinevich, Andrew F. *7 Deadly Scenarios.* New York: Bantam Dell, 2009.

Liff, Adam P. "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio." *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* Vol. 22, No. 3 (2013): http://dx.doi.org/10.1080/09636412.2013.816122.

Lynn III, William J. "Defending a New Domain." *Foreign Affairs* Vol. 89 Issue 5 (September/October 2010): 97-108.

Milevski, Lucas. "Stuxnet and Strategy: A Special Operation in Cyber Space?" *Joint Forces Quarterly*, Issue 63, 4th Quarter 2011: 64-69. http://www.ndu.edu/press/stuxnet-and-strategy.html.

Miller, Robert A. and Daniel T. Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," *Defense Horizons*, Number 68 (September 2009), 1-6. http://www.ndu.edu/CTNSP/docUploaded/DH68.pdf.

Milt Priggee National Cartoons Collection. MiltPriggee.com. http://www.miltpriggee.com/cartoons/national/view/9407/.

Pape, Robert A. "The True Worth of Air Power." Foreign Affairs. March/April 2004. Accessed December 13, 2014. http://www.foreignaffairs.com/articles/59714/robert-a-pape/the-true-worth-of-air-power.

Peterson, Dale. “Offensive Cyber Weapons: Construction, Development, and Employment.” *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).

Reed, Thomas C. *At the Abyss: An Insider’s History of the Cold War*. New York, NY: Ballantine Books, 2007. Kindle edition.

Rid, Thomas. *Cyber War Will Not Take Place.* New York: Oxford University Press, 2013.

Rid, Thomas. “More Attacks, Less Violence,” *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).

Rustici, Ross M. “Cyberweapons: Leveling the International Playing Field,” *Parameters* (Autumn 2011): 32-42. http://lomc.idm.oclc.org/login?url=http://search.proquest.com/docview/928971315?accountid=14746.

Santayana, George. *The Life of Reason.* 5 vols. New York, NY: Dover Publications, 1980. http://www.gutenberg.org/files/15000/15000-h/vol1.html.

Shakarian, Paolo. “The 2008 Russian Cyber Campaign Against Georgia.” *Military Review* (November-December 2011): 63-68. http://lomc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=67643241&site=ehost-live.

Shakarian, Paolo. “Stuxnet: Cyberwar Revolution in Military Affairs.” *Small Wars Journal,* April 15, 2011.

Stone, John. “Cyber War *Will* Take Place!” *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013).

Tzu, Sun. *The Art of War*, Edited by Samuel B., Griffith. Translated by Samuel B., Griffith. New York, NY: Oxford University, 1971.

U.S. Department of Defense. *Cyberspace Operations.* Joint Publication 3-12 (R). Washington, DC: Department of Defense, February 5, 2013.

Warner, Edward. “Douhet, Mitchell, Seversky: Theories of Air Warfare.” In *Makers of Modern Strategy*, edited by Edward Mead Earle, 485-503. Princeton, NJ: Princeton University Press, 1943.

Warner, Michael. “US Policy in Cyberspace.” Lecture presented at Marine Corps University, Quantico, VA, January 2015.

Werrell, Kenneth P. *Archie to SAM : A Short Operational History of Ground-based Air Defense*. Maxwell Air Force Base, Ala: Air University Press, 2005. *eBook Collection (EBSCOhost)*, EBSCO*host* (accessed March 30, 2015).