Do the Principles of War Apply to Cyber War?

A Monograph
by
Major David B Farmer
USAF

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

AY 2010

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-MAY-2010	SAMS Monograph	July 2009 – May 2010

4. TITLE AND SUBTITLE

Do the Principles of War Apply to Cyber War?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major David B. Farmer (U.S. Air Force)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
250 Gibbon Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Foreign Military Studies Office & Command and General Staff College
Director, FMSO
731 McClellan Ave.
Fort Leavenworth, KS 66027-1350

10. SPONSOR/MONITOR'S ACRONYM(S)
SAMS

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this monograph is to examine whether the Principles of War, as defined within the U.S. military's *Joint Publication 3-0, Joint Operations,* can be applied to cyber war. Since 2005, the U.S. military recognized cyber conflict as a new domain for conducting military operations. Consequently, in order to ensure future success on the battlefield, commanders need to understand cyberspace operations and how these operations fit within the Principles of War.

The methodology of this paper is to first examine, and subsequently show the history of the Principles of War in order to provide a context from which military personnel can then categorize cyberspace within the historic model. Such an examination is relevant because not only is U.S. cyber policy and strategy currently being developed, but the United States is also standing up a United States Cyber Command for the first time in history. Having discussed the Principles of War and woven them across an understanding of cyber operations, one can then see that the current Principles of War do in fact apply to cyber war. There is no need to create new Principles of War that apply exclusively to the cyber domain.

15. SUBJECT TERMS
Principles of War, Cyber War, Information War, Computer Network Attack, Cyber Crime, Cyberspace

16. SECURITY CLASSIFICATION OF: (U)			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Stefan J. Banach COL, U.S. Army
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	60	913-758-3302

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major David B Farmer

Title of Monograph: Do the Principles of War Apply to Cyber War?

Approved by:

_____ Gerald S. Gorman, PhD	Monograph Director
_____ James Tennant, COL, SF	Monograph Reader
_____ Stefan Banach, COL, IN	Director, School of Advanced Military Studies
_____ Robert F. Baumann, Ph.D.	Director, Graduate Degree Programs

Abstract

DO THE PRINCIPLES OF WAR APPLY TO CYBER WAR, by Major David B. Farmer, United States Air Force, 60 pages.

The purpose of this monograph is to examine whether the Principles of War, as defined within the U.S. military's *Joint Publication 3-0, Joint Operations,* can be applied to cyber war. Since 2005, the U.S. military recognized cyber conflict as a new domain for conducting military operations. Consequently, in order to ensure future success on the battlefield, commanders need to understand cyberspace operations and how these operations fit within the Principles of War.

The methodology of this paper is to first examine, and subsequently show the history of the Principles of War in order to provide a context from which military personnel can then categorize cyberspace within the historic model. Such an examination is relevant because not only is U.S. cyber policy and strategy currently being developed, but the United States is also standing up a United States Cyber Command for the first time in history. Having discussed the Principles of War and woven them across an understanding of cyber operations, one can then see that the current Principles of War do in fact apply to cyber war. There is no need to create new Principles of War that apply exclusively to the cyber domain.

TABLE OF CONTENTS

ILLUSTRATIONS

Introduction

> The form of any war--and it is the form which is of primary interest to men of war--depends on the technical means of war available
>
> Giulio Douhet[1]

A core responsibility of the U.S. government is to protect the American people – in the words of the framers of our Constitution, to "provide for the common defense." Over the past decade, a discussion on the application of cyber war capabilities has become increasingly prominent due primarily to the fact that as many as 120 international governments are pursuing information warfare programs.[2] In response to other nation-states' cyber programs, the *2006 Quadrennial Defense Review* (QDR) requested that the Department of Defense (DoD) develop a capability to shape and defend cyberspace.[3] In keeping with this directive and breaking paradigms of the past, the *2006 QDR* became one of the first official DoD documents to highlight the need to develop a new operational domain dubbed "cyberspace." Advocating military preparedness in the domains of air, land, sea, and space, the authors of the *2006 QDR* also highlighted the criticality of preparing forces to fight and win in the realm of cyberspace.[4] Based on the requirement to operate in all domains, the U.S. military needs to discern if the current Principles of War apply to cyber war. Is there a need to develop new Principles of War to address the challenges of cyber war? If so, to what extent does the United States need to reshape its armed forces to meet such challenges to ensure freedom of maneuver in the cyber domain?

---

[1] Giulio Douhet, *Command of the Air*, trans. Dino Fer-ari (New York: Coward-McCann, 1942).

[2] Owen Davies, Stephen Steele, Cynthia Ayers and Marvin Cetron, "World War 3.0: Ten Critical Trends for Cybersecurity," *The Futurist* (September 2009): 40.

[3] *Quadrennial Defense Review 2006* (Washington D.C.: Secretary of Defense, 2006), 32.

[4] Ibid, 37.

The world has seen an increase in state and non-state actors utilizing cyber war techniques against the United States, in both a domestic and military application.[5] Systems defense with deployed intrusion detection and prevention mechanisms is quite a different matter than the employment of "malicious code"[6] intended to incapacitate command and control systems. In the past, the military has seen the cyber war as only a support function and not as a tool a commander can use for operations. After reviewing U.S. joint doctrine, one can see that cyber war has continually been relegated to a supporting role. In fact, *Joint Publication 3-0, Joint Operations* specifically does not mention cyber war.[7] The only reference one finds for cyber war terminology is in supporting joint publications such as *Joint Publication, 6-0, Joint Communications Systems*[8] and *Joint Publication, 3-13, Information Operations*.[9] Consequently, the U.S. military needs to develop within joint doctrine a common and comprehensive definition for the application of cyber war.

In the block quote at the beginning of this monograph, General Douhet referred to the application of air power technology. General Douhet speculated that sometimes technology represents not only a revolution in military affairs, but also perhaps a military revolution. In *The Dynamics of Military Revolution 1300-2050*, MacGregor Knox and Williamson Murray defined a military revolution as having sweeping impacts on not only the battlefield, but also within society. Using this definition in their research, the authors identified five military revolutions

---

[5] A.J. Bosker, "SECAF: Dominance in cyberspace is not optional," *Air Force Print News*, May 2007.

[6] **Malicious Code:** Software designed to infiltrate a computer system without the owner's informed consent. Lt Col Shane Courville, *Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future*, Occasional Paper No. 63. (Maxwell AFB, AL: Center for Strategy and Technology, December 2007), 42.

[7] *Joint Publication 3-0 Joint Operations: 17 September 2006, Incorporating Change 1* (Washington D.C.: Joint Chiefs of Staff, February 13, 2008).

[8] *Joint Publication 6-0 Joint Communications System* (Washington D.C.: Joint Chiefs of Staff, March 20, 2006), I-11.

[9] *Joint Publication 3-13 Information Operations* (Washington D.C.: Joint Chiefs of Staff, February 13, 2006), I-7.

through history.[10] In a more narrowly focused definition, Knox and Murray then defined a revolution in military affairs as a capability or improvement that has an impact only on the battlefield and does not extend into other societal domains. While technological and doctrinal advances may represent revolutions in military affairs, the creation of the modern nation-state, for example, clearly qualifies as a more significant military revolution.[11] As cyber war grows increasingly more prevalent and critical to survival, one must recognize its significance. Essentially, U.S. leaders must discern if the world stands on the precipice of a life-altering military revolution or merely a revolution in military affairs.

Just as General Douhet referred to technology with respect to airpower as military revolution, the author of this monograph contends that cyber war represents a change in warfare with far-reaching effects beyond the battlefield. Like Knox and Murray's military revolution, cyber technology has influenced all aspects of society under the guise of an information revolution. Considering only the amount of data exchanged or transmitted during a military conflict, the world has seen an increase from 100 words per minute in Vietnam to over 1.5 trillion words per minute during Operation IRAQI FREEDOM.[12] However, even beyond a military context, this nation cannot perform the most basic functions without unencumbered access to cyberspace. Given the impacts to society and the increasing information requirements in our military today, we stand in the midst of a new military revolution.

---

[10] **Knox and Murray identified Military Revolutions:** 1) Creation of the modern nation-state, 2) French Revolution, 3) Industrial Revolution, 4) World War I and 5) the advent of nuclear weapons. MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution 1300-2050* (Cambridge: Cambridge University Press, 2001), 6.

[11] Ibid, 6.

[12] *Joint Operations Insights and Best Practices* (Norfolk: Joint Warfighting Center, July 2008), 8.

In 2005, Colin S. Gray published *The American Way of War* in which he identified twelve specific characteristics on how America fights its wars.[13] From these characteristics, Gray identified that, "America is the land of technological marvels and of extraordinary technology dependency . . . American soldiers say that the human beings matter most, but in practices, the American way of war, past, present, and prospectively future, is quintessentially and uniquely technologically dependent."[14] If the U.S. is truly a technologically dependent military, then it needs to address all aspects of war dealing with technology, to include cyber war, in planning.

In providing for the common defense of the American people, the U.S. military organizes based on certain fundamentals to ensure success of joint operations. The Principles of War provide an insight into our understanding of these fundamentals of military operations. Cyber war, as an on-going military revolution, might drastically impede the U.S. government and military from achieving national objectives in the future. Consequently, U.S. military officials must assess how to best organize and equip to address this 21st century challenge. As a guide for efficacy, U.S. military leaders have traditionally utilized the Principles of War to ensure readiness. Therefore, military officials must ask whether the Principles of War, as written in joint doctrine, apply to cyber war.

The methodology used to determine whether the Principles of War are applicable to cyber war and whether or not U.S. officials must revise these time-tested precepts will accomplish a number of tasks. This monograph first elaborates on the Principles of War using current joint U.S. doctrine and looks at how the Principles of War came into existence. Next, the

---

[13] **Gray's 12 characteristics of the American Way of War**: 1) Apolitical, 2) Astrategic, 3) Ahistorical, 4) Problem-solving, optimistic, 5) Culturally ignorant, 6) Technologically dependent, 7) Firepower focused, 8) Large-scale, 9) Profoundly regular, 10) Impatient, 11) Logistically excellent and 12) Sensitivity to casualties. Colin S. Gray, *The American Way of War* (Reading: University of Reading, 2005), 28-29.

[14] Gray, 29.

study defines common cyber war terms to establish a beginning reference point for future analysis. After examining these two concepts, the paper then compares and analyzes both in order to determine whether the existing structure and content of the Principles of War adequately address the nature of cyber war. Some theorists believe that cyber war does not fit within the Principles of War model identified in *Joint Publication 3-0*. In his book *The Principles of War for the Information Age*, Robert Leonhard argued that the Principles of War do not apply to cyber war and that new Principles of War should be created.[15] The author of this monograph will address some of Leonhard's contentions in the following chapters and challenge his argument that cyber war does not fit within *Joint Publication 3-0*. A common understanding of these complex issues allows commanders and leaders to more effectively conduct operations within the cyber war domain. Having reviewed the Principles of War and concepts associated with the cyber domain, the reader should understand that the Principles of War do apply to cyber war and there is no need to develop additional principles.

[15] Robert Leonhard, *The Principles of War for the Information Age* (Novato, CA: Presidio Press, 2000), vii.

What are the Principles of War?

> An irresolute general who acts without principles and without plan, even though he lead an army numerically superior to that of the enemy, almost always finds himself inferior to the latter on the field of battle. Fumblings, the middle course, lose all in war.
>
> Napoleon[16]

Military theorists, such as Clausewitz, Jomini and Fuller, have attempted to identify the Principles of War so armies can train and equip their forces based on proven precepts and subsequently enjoy success on the battlefield. General Carl von Clausewitz defined a principle as a "law for action but not in its formal definitive meaning. It represents only the spirit and the sense of the law. A principle is objective if it rests on truth and if it is subjective, it generally called a maxim and therefore has value only for the person who adopts it."[17] Unlike other theorists, Clausewitz did not explicitly outline Principles of War; however, one can definitely identify certain concepts that Clausewitz felt important in the conduct of war. Clausewitz avoided lists of undisputable and dogmatic axioms, but did believe that certain principles could be effectively employed as tests for military efficacy. Additionally, Clausewitz contended that any derived principles most often applied to tactics, but only rarely to strategy.

Merriam-Webster Online defines a principle as a comprehensive and fundamental law, doctrine, or assumption.[18] Merriam-Webster differs from Clausewitz in that a principle is given as a law; the definition is more in line with how Baron Antoine de Jomini would define a principle.

---

[16] Lt Col Charles Westenhoff, *The CADRE Digest of Air Power Opinions and Policy Issues* (Maxwell AFB, AL: Air University, October 1990), 66.

[17] Carl von Clausewitz, *On War*, translated and edited by Michael Howard and Peter Paret (West Sussex: Princeton University Press, 1976), 151.

[18] *Merriam-Webster Online*, s.v. "Merriam-Webster Online," http://www.merriam-webster.com (accessed March 22, 2010).

Jomini wrote, "It is proposed to show that there is one great principle underlying all the operations of war,—a principle which must be followed in all good combinations."[19]

Although most military officials may indicate that a list of variables, like the Principles of War, may exhibit a Jominian influence, this monograph uses a definition closer to Clausewitz's assertions. With this in mind, this paper explores the Principles of War as guiding precepts that support military logic and not draconian axioms that must be followed dogmatically. With that understanding, this monograph now proceeds by outlining how the current principles have evolved over time and then describing the individual Principles of War.

History of the Principles of War

Throughout history, military strategists and theorists have identified techniques they felt an army needs to ensure success on the battlefield. As new technology has become available, people have often challenged and, at times, changed these techniques in order to make them more relevant. Regardless of the deletion and addition of certain precepts, there are a few concepts that have withstood the test of time. The more enduring concepts have evolved into the current Principles of War. While a particular practice may have lasted due to certain environmental conditions, a principle demonstrates a more enduring capacity. History shows that some of the Principles of War remain constant through time despite the introduction of new technology or military revolutions. To show these constant principles, this paper breaks down the evolution of the Principles of War from early theory, through the Age of Enlightenment, and to the 20th century.

[19] Baron Antoine de Jomini, *The Art of War*, trans. Capt G.H. Mendall and Lt W.P. Craighill (West Point: US Military Academy, 1862), 71.

Early Theory

In his work *The Art of War*, Sun Tzu was one of the earliest theorists to identify what armies must do to be successful in the conduct of warfare. Similar to today's doctrinal references, Sun Tzu included "how to" chapters on basic ideas dealing with maneuver, ground formations, and planning attacks.[20] Sun Tzu's definitions of these basic ideas are similar to some of the definitions in current U.S. doctrine outlining the Principles of War. For example, Sun Tzu wrote that upon maneuvering forces, one should place his enemy in a position of disadvantage through flexible application of combat power.[21] Although Sun Tzu did not specifically state that maneuver was an enduring principle of war, his teachings highlighted the importance of the concept. In other words, Sun Tzu did not explicitly provide a list of precepts, but his writings certainly laid an intellectual foundation from which one can draw such principles. Theorists, such as Clausewitz and Jomini, in the 18th and 19th century used theorists, such as Sun Tzu, as the basis for their research on the conduct of war.[22]

About the same time as Sun Tzu, the Greeks sought to master the Principles of War to defend Greece from the Persian armies. In *The History of the Peloponnesian War*, Thucydides provided one of the earliest examples of military writings that contained principal-based aspects. Thucydides was a Greek General who wanted to capture the history of the Peloponnesian War to provide written documentation from which to derive certain principles from Greek battles. Similarly, another Greek writer, Herodotus, captured Greek experience in battles in *The Histories*. Herodotus wrote a detailed account of the Battle of Marathon, which highlighted the criticality of

---

[20] Sun Tzu, *On the Art of War*, trans. Lionel Giles, 1910, http://www.au.af.mil/au/awc/awcgate/artofwar.htm#7 (accessed 14 January 2010).

[21] Ibid.

[22] Maj Walter Piatt, "Do the Principles of War Still Apply?" (master's thesis, School of Advanced Military Studies, 1999), 4.

principles like mass and economy of force.[23] These two early Greek authors wrote from primarily historical perspectives, but as one reads the material, one can identify basic principles that are similar to, and often lay the foundation for, today's Principles of War.

Unlike Jomini or General Fuller, none of the early theorists explicitly outlined their Principles of War as currently depicted in doctrine; however, from their writings one can see that these early theorists did explore critical concepts and fundamentals that would involve into the documented Principles of War in use by militaries today. Early theorists provided the historical baseline for theorists of the future to use in developing their principles of war.

Age of Enlightenment

During the Age of Enlightenment, Western Europeans reinvigorated their study of history to understand basic military skills. Nation-states were growing in size and the armies of the period tried to understand how to take virtuosity in war at the tactical level to the operational or strategic level. In doing so, theorists again contributed to a body of knowledge from which militaries would eventually draw the Principles of War. Due to environmental changes within societies, armies grew from homogenous small professional armies to large conscript armies throughout Europe.[24] As armies grew larger, command and control as well as the training of the forces became increasingly difficult; theorists of the time focused on how best to address these challenges. As discussed earlier, two of the most important theorists during this period were Baron Antoine de Jomini and Major General Carl von Clausewitz.

After studying Napoleon, Jomini became one of the first Western Europeans to annotate basic principles that most closely resemble the modern Principles of War. Jomini tried to capture

---

[23] *Introduction to the Principles of War and Operations* (University of California Military Science, 2009), 172.

[24] Michael Howard, *Clausewitz: A Very Short Introduction* (New York: Oxford University Press, 2002), 11.

the military genius of Napoleon so other militaries could replicate his resounding successes. Jomini's writings were translated globally and most armies of the 19th century, including the United States military, adopted his concepts within their respective doctrinal references.[25]

Jomini summarized the Principles of War using four maxims. The first was to project the mass of an army by strategic movements, successively, upon both the decisive points of a theater of war and upon the communications of the enemy as much as possible without compromising one's own capabilities. The second maxim was to maneuver to engage fractions of the hostile army with the bulk of one's forces. The third maxim was to maneuver the mass of forces upon the decisive point or upon that portion of the hostile line that it is of the first importance to overthrow. The fourth maxim was to ensure that the massing of forces should not only be thrown upon the decisive point, but should also engage at the proper time and with the requisite energy.[26] From these maxims come the *Joint Publication 3-0* basic principles of mass, objectives, offensive, maneuver, surprise and security.

While Jomini saw war as a science, Clausewitz, Jomini's contemporary, viewed war at the strategic level as an art.[27] Clausewitz began to study warfare after the Prussian loss at the battle of Jena-Auerstedt in 1806 against Napoleon. From his reflection and research, Clausewitz first published his findings in 1812 under the title *Principles of War*.[28] The principles that Clausewitz identified in his 1812 publication were his first attempt to develop a training aide for rebuilding the Prussian army. Clausewitz listed his principles as offense, defense, governing the

---

[25] *Introduction to the Principles of War and Operations* (University of California Military Science, 2009), 172.

[26] Jomini, *The Art of War*, 71.

[27] Howard, *Clausewitz: A Very Short Introduction*, 33.

[28] Carl Von Clausewitz, *The Principles of War*, trans. Hans W. Gatzke, http://www.clausewitz.com/readings/Principles (accessed 14 January 2010).

use of troops, and use of terrain.[29] *Principles of War* was the precursor to Clausewitz's *On War* that outlined not only the basics of how to fight at the tactical level, but also how to consider the conduct of war at the strategic level.[30]

20th Century

In 1903, Marshal Ferdinand Foch of France published a book called *The Principles of War* as an abstract of Clausewitz's ideas.[31] Foch reviewed successful campaigns of the 19th century, such as those of Moltke, to develop his principles. Foch's *The Principles of War* was a collection of lectures that reintroduced the concept of the offensive to French military theory.[32] Foch identified principles such as economy of force, maneuver, security, surprise, and the decisive attack as enduring concepts critical to the success of the French military.[33] As a testament to this author's significant influence, the principles developed by Foch became the baseline for French officers to train and operate during World War I.

The Industrial Revolution and World War I created new challenges for the conduct of war. Knox and Murray wrote that combatants involved in World War I had to deal with an increase in the size of the battlefield, witnessed the mobilization of mass armies, and experienced the devastating impact of new and more lethal technology. Such changes in the way war was fought also brought about some societal changes. From their analysis, Knox and Murray identified World War I as one of only five military revolutions throughout history.[34] After the war, military leaders reflected on the experience of World War I, especially with regard to their ability to command and control armies in battle. Because of their reflections, some of these

---

[29] Ibid.
[30] Howard, *Clausewitz: A Very Short Introduction*, 33.
[31] Ibid.
[32] Marshall Ferdinand Foch, *The Principles of War*, trans. Hillaire Belloc (New York: Henry Holt and Company, 1903), v.
[33] Ibid, xi.
[34] Knox and Murray, 6.

leaders (e.g. Foch and Fuller) endeavored to outline their basic principles in order to ease the rapid mobilization of forces as well as facilitate the command and control of large armies needed for future wars.

British Major General J.F.C. Fuller wrote in his book, *The Foundations of the Science of War*, the original nine Principles of War that became the bedrock for contemporary joint operations. The principles that General Fuller identified were objective, offensive, mass, economy of force, movement, surprise, security and cooperation. Fuller also identified three tactical Principles of War that he referred to as demoralization, endurance, and shock.[35] Based on his formative experiences during World War I, Fuller attempted to identify what went wrong to better inform militaries of the future.[36]

Because of Fuller's research, the British became the first nation to document their Principles of War in formal doctrine.[37] Based predominantly on Fuller's concepts, British officials published in 1920 the Principles of War, as outlined in *British Field Service Regulations (Provisional),* and included maintenance of the objective, offensive action, surprise, concentration, economy of force, security, mobility and co-operation. [38]

In 1921, Fuller's principles first appeared in U.S. doctrine in *Training Regulations, 10-5*.[39] Based largely on the British field publication and Fuller's precepts, the principles identified in this document were objective, offensive, mass, economy of force, movement,

---

[35] Piatt, 52.

[36] J.F.C. Fuller, *The Foundations of the Science of War (Reprint).* (Ft Leavenworth: CGSC Press, 1993), 220.

[37] John Alger, "The Origins and Adaptation of the Principles of War" (master's thesis, Command General Staff College, 1995), iv.

[38] Ibid, iv.

[39] David Burwell, "Morale As A Principle of War" (master's thesis, School of Advanced Military Science, 2000), 10.

surprise, security, simplicity and cooperation.[40] These nine Principles of War remained in U.S. doctrine until their disappearance in the 1930s as officials questioned their validity primarily due to the introduction of new technology such as airpower and armor. Influenced not only by new technology, but by also funding constraints due to the Great Depression, military leaders lost focus on the Principles of War until their rediscovery years later.

In 1949, the Principles of War reappeared in U.S. doctrine as *Field Manual, 100-5 Field Service Regulations: Operations*.[41] The principles identified in that document are basically the same as those currently published in *Joint Publication 3-0*. However, the difference from the 1921 list and these later publications is that military officials replaced cooperation with unity of command and changed mobility to maneuver. Although the terminology of both cooperation and mobility changed to better reflect the existing lexicon of the forces at the time, the overall content of the concepts remained intact.

In 1976, authors of *Field Manual 100-5* signaled their impression of the irrelevance of the Principles of War, based on lessons learned from Vietnam and the Cold War, by removing the concept from U.S. doctrine.[42] In the 1983 revision of *Field Manual 100-5*, authors reincorporated the Principles of War back into U.S. doctrine to augment their description of the now famous Air Land Battle doctrine.[43]

Over the years, the nine principles that Major General Fuller initially identified have morphed into the current principles represented in *Joint Publication 3-0*. In outlining how each of the current military services conducts operations, each of the respective service documents reflect the basic Principles of War identified in joint doctrinal references. Highlighting how the current

---

[40] Piatt, 53.
[41] Ibid, 24.
[42] Ibid, 26.
[43] Ibid, 27.

Principles of War identified in *Joint Publication 3-0* pervade each service, Figure 1 shows which baseline documents incorporate the Principles of War.

	Joint	Army	Navy	Air Force	Marines
Document	JP 3-0, Operations	FM 3-0, Operations	NWP 3 Series, Operations	AFDD 1, Air Force Basic Doctrine	MCDP 1-0, USMC Operations

Figure 1: Service Doctrine Referencing Principles of War

U.S. Principles Defined

Carl von Clausewitz defined war as "… an act of force to compel our enemy to do our will."[44] This definition is the foundational basis for the development of *Joint Publication 3-0* that serves as the primary reference for conducting operations within the U.S. military. As outlined by the *U.S. National Security Strategy*, the military must not only provide for the common defense but also ensure that the nation can compel enemies to act in a way that best achieves U.S. national objectives. In presenting the basic tenets for conducting joint operations, authors of *Joint Publication 3-0* give the nine basic principles, adding three additional tenets; authors added restraint, perseverance and legitimacy as principles in order to more holistically capture what is required for the successful conduct of joint operations in the contemporary operating environment.[45] These additional principles have the same weight in joint operations as do the historical Principles of War. For reference, the definitions of the U.S. Principles of War from *Joint Publication 3-0* can be found in Appendix B.

[44] Clausewitz, *On War*, 75.
[45] *Joint Publication 3-0*, II-1.

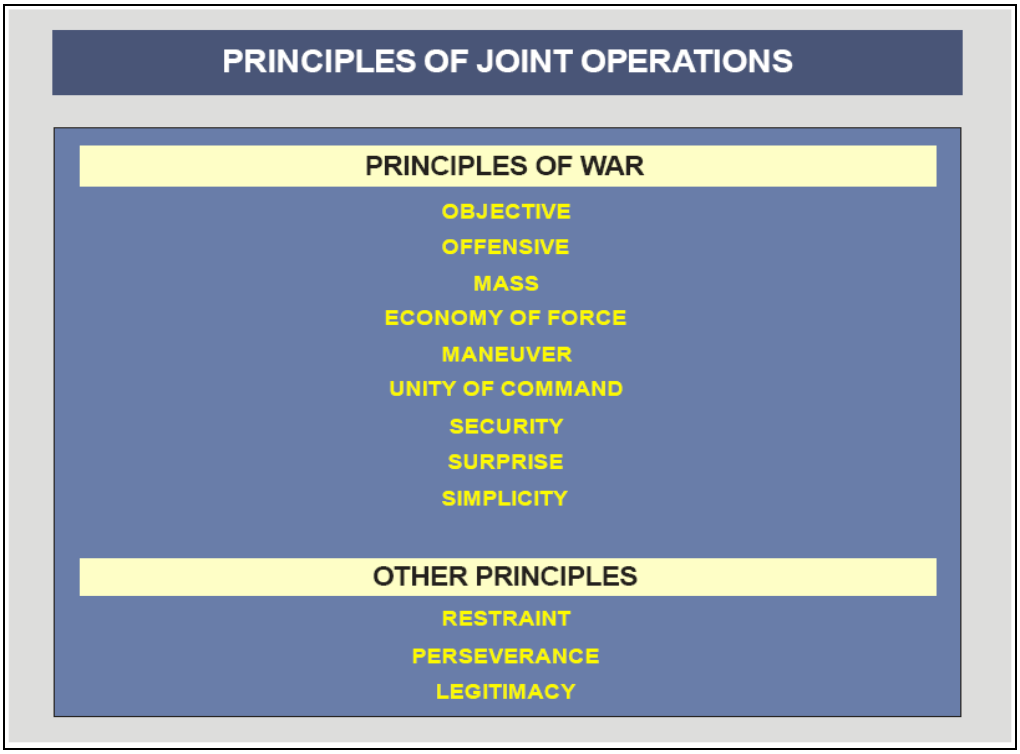

Figure 2: Joint Publication 3-0, Joint Operations principles

Other Nations' Principles of War

Nations throughout the world continue to develop Principles of War for their militaries in order to achieve successful results on the battlefield. Figure 3 highlights the Principles of War that different nations currently use in their militaries. This chart not only underscores the diversity among nations over supposedly universal principles but also highlights the need for the U.S. military to coordinate with coalition nations to ensure a common understanding of how best to achieve success in the conduct of war. For the purpose of this monograph, the differences in the Principles of War between nations add a degree of difficulty to the integration of any understanding of cyber war. For example, although each nation abides by the principle of surprise, only the United States and China use the principle of unity of command. Without unity of command, what principle will then guide the coordination of U.S. cyber forces with other nations?

UNITED STATES	GREAT BRITAIN AUSTRALIA	FORMER SOVIET UNION	FRANCE	PEOPLE'S REPUBLIC OF CHINA
Objective	Selection & Maintenance of Aim			Selection & Maintenance of Aim
Offensive	Offensive Action			Offensive Action
Mass	Concentration of Force	Massing & Correlation of Force	Concentration of Effort	Concentration of Force
Economy of Force	Economy of Force	Economy, Sufficiency of Force		
Maneuver	Flexibility	Initiative		Initiative & Flexibility
Unity of Command	Cooperation			Coordination
Security	Security			Security
Surprise	Surprise	Surprise	Surprise	Surprise
Simplicity				
	Maintenance of Morale	Mobility & Tempo Simultaneous Attack on All Levels, Preservation of Combat Effectiveness, Interworking & Coordination	Liberty of Action	Morale, Mobility, Political Mobilization, Freedom of Action
Adapted from JT Pub 1, FM 100-1, AFM 1-1, and FMFM 6-4				
Military Review, May 1955, and Soviet Battlefield Development Plan				

Figure 3: Comparative Chart of Other Nations' Principles of War[46]

The history of the Principles of War shows that they are not just one man's idea, but represent an amalgamation of many ideas, evolved over centuries of refinement, by multiple theorists (e.g. Jomini, Foch, Clausewitz, Fuller, etc). The durability of the Principles of War is a testament to their utility. The principles are defined broadly enough to make them applicable to today's operating environment and yet specific enough to be applied at every level of war. The explanations provided above for the Principles of War serve as the baseline to later consider their application with respect to cyber war. Since the Principles of War are the foundation from which the U.S. military conducts successful military operations, understanding the development of these principles prepares us for the following discussion. However, prior to conducting such an analysis and then drawing conclusions, a reader must possess a full understanding of cyber war. Since the concept of cyber war is inadequately explained in U.S. doctrine, a deliberate exploration of the concept is especially warranted.

[46] *Joint Staff Officers Guide Publication 1.* (Norfolk: Armed Forces Staff College, 1997).

What is Cyber War?

> We should base our security upon military formations which make maximum use of science and technology in order to minimize numbers of men.
>
> Dwight D. Eisenhower[47]

Defining cyber war is a challenge. Commanders in the past have seen the application of cyber war as only a supporting mechanism and not as a direct tool to be used in the conduct of operations. Upon reviewing joint doctrine, one can subtly witness how the military community currently relegates cyber war to a support function. In fact, *Joint Publication 3-0, Joint Operations*[48] and *Joint Publication 5-0, Joint Operation Planning,*[49] the capstone training and operational documents of the U.S. military do not specifically mention cyber war. The only reference one finds to the terminology of cyber war is contained within supporting doctrine such as *Joint Publication, 6-0, Joint Communications Systems*[50] and *Joint Publication, 3-13, Information Operations*.[51] Additionally, when assessing national security documents, the current *2006 National Security Strategy* [52] does not address cyber threats at the level of national strategy. *The National Strategy to Secure Cyberspace,* published in 2003, is the only whole-of-government document dedicated to addressing cyber challenges at this time.[53] Splitting the role of cyber defense between the Department of Homeland Security (DHS) and the DoD, authors of *The National Strategy to Secure Cyberspace* detract from the very notion of unity of command

---

[47] Westenhoff, *The CADRE Digest of Air Power Opinions and Policy Issues*, 56.

[48] *Joint Publication 3-0*.

[49] *Joint Publication 5-0 Joint Operating Planning* (Washington D.C.: Joint Chiefs of Staff, December 26, 2006).

[50] *Joint Publication 6-0*, I-11.

[51] *Joint Publication 3-13*, I-7.

[52] *The National Security Strategy of the United States of America* (Washington D.C.: The White House, 2006).

[53] *National Strategy to Secure Cyberspace* (Washington D.C.: White House, February 2003).

ironically heralded within *Joint Publication 3-0*.[54] This disjointed guidance leads to a lack of common understanding of cyber operations inside the military community. This chapter presents the severely underdeveloped and disjointed understanding of cyber war that currently exists within the DoD in order to establish a common knowledge base for further analysis.

A New Domain

Joint Publication 3-0 defines the operational environment as "the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment."[55] Additionally, doctrine currently lists only air, land, maritime and space as the domains in which the U.S. military operates. Since the release of this joint publication in 2006, the definition of the operational environment has expanded within DoD strategic planning documents to include cyber as a domain for operations in addition to air, land, sea and space.

The inclusion of cyber as an operating domain is first referenced in joint documentation starting in 2005 with the publication of the *Capstone Concept for Joint Operations*.[56] As with the other capstone documents preceding it, the 2005 document headed the family of joint operational concepts that describe how joint forces are expected to operate across the range of military operations in 2012-2025. Its purpose was to lead force development and employment primarily by providing a broad description of how the future joint force should expect to operate.[57]

---

[54] Ibid.
[55] *Joint Publication 3-0*, xvi.
[56] *Capstone Concept for Joint Operations* (Washington D.C.: Chairman of the Joint Chiefs of Staff, August 2005), 7.
[57] Ibid, vii.

By including in the 2005 *Capstone Concept for Joint Operations* the notion of cyber as a separate domain, authors directly influenced the incorporation of the largely ignored concept in the *2006 QDR* as well. The *2006 QDR* defined the domains of an operational environment as air, land, maritime, space and, for the first time, cyberspace.[58] Since the purpose of the *QDR* has traditionally been used to define the current status of the DoD and where the DoD believed that it needed to go, the inclusion of cyberspace was viewed by many as a significant step forward.[59] More importantly, the *QDR* was the first DoD document that focused funding on cyber war capabilities and became the baseline document for future funding, program, and force composition for all cyber related entities and activities.

Today, current strategic planning documents, to include the *Capstone Concept for Joint Operations 2009*,[60] the *Joint Operating Environment 2008*[61] as well as the *Quadrennial Defense Review 2010*[62] maintains cyber as a domain for operations. Cyber has earned permanent integration into U.S. military strategic planning documents to address foreseeable conflicts. Joint doctrine needs to catch up with these strategic planning documents in including cyber as a domain in future publications.

The cyber domain is unique for several reasons. First, unlike the long standing physical qualities (air, water, terrain) that define the other domains, the cyber arena is defined largely by manufactured technological artifacts. Second, unlike the relatively finite borders of the traditional

---

[58] *Quadrennial Defense Review 2006* (Washington D.C.: Secretary of Defense, 2006), 37.
[59] Ibid, iii.
[60] *Capstone Concept of Joint Operations v 3.0* (Washington D.C.: Chairman of Joint Chiefs of Staff, 15 Jan 2009), iv.
[61] *Joint Operating Environment 2008* (Norfolk: United States Joint Forces Command, November 25, 2008), 44.
[62] *Quadrennial Defense Review 2010* (Washington D.C.: Secretary of Defense, February 2010).

land, sea, air, and space battlespaces, the cyber arena crosses the spectrum of the other domains.[63] Although predominantly an artificial or manmade domain, the cyber battlespace does exhibit some natural aspects like the more traditional battlespaces. For example, the cyber domain requires man to provide the hardware for transmission and receipt of data. Additionally, the cyber domain uses elements of the naturally occurring electromagnetic spectrum. However, just like the traditional air domain, one still needs manufactured hardware to take advantage of it. Figure 4 highlights the three elements of the cyber domain, breaking the domain down by the electromagnetic spectrum, electronic systems and physical infrastructure.[64] The cyberspace domain is the region where these three areas overlap. Of note for this monograph, the cyber domain does possess naturally occurring characteristics like the traditional domains of land, sea, and air. However, military officials must consider this battlespace unique from the perspective that it is highly dependent on artificial or manmade hardware for its existence.

[63] Lt Col Joseph Scherrer and Lt Col William Grund, *A Cyberspace Command and Control Model* (Montgomery, AL: Air University Press, 2009), 9.

[64] *Air Force Doctrine Document 2-X: Cyberspace Operations (Draft)* (Washington D.C.: Department of the Air Force, 2009), 1.

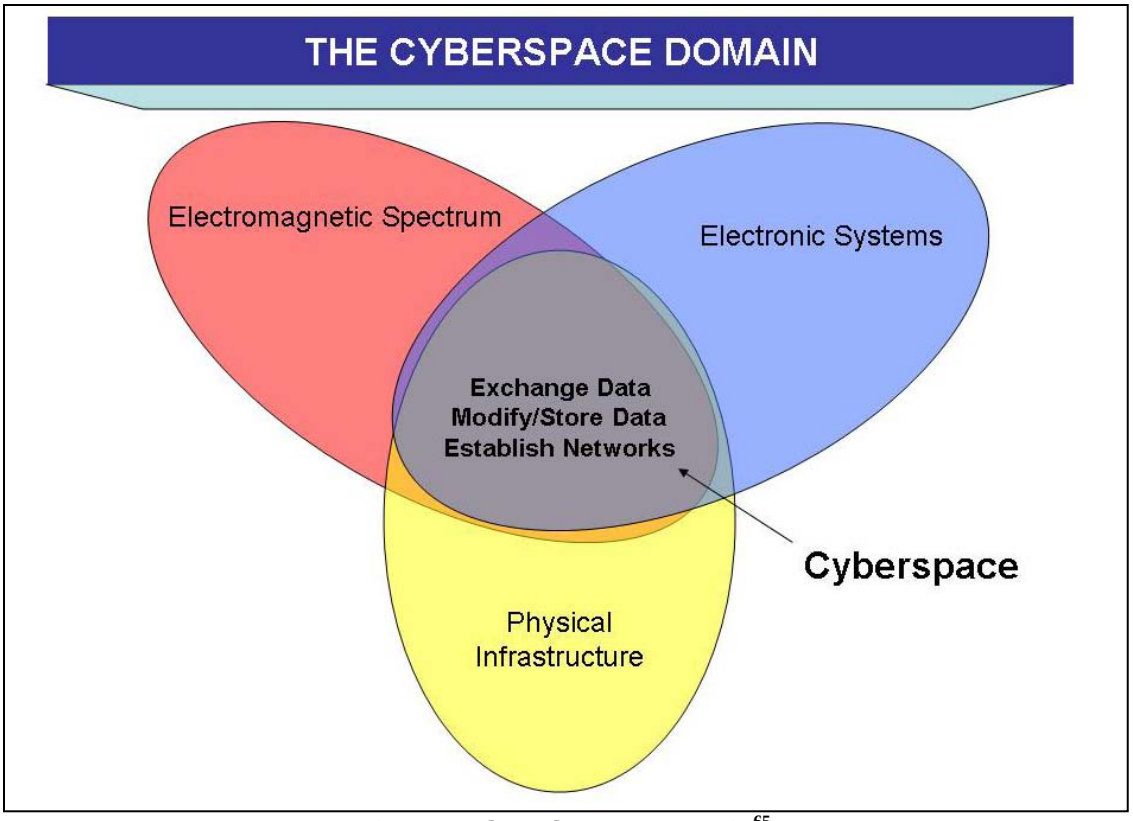

Figure 4: The Cyberspace Domain[65]

Cyberspace

The DoD currently defines cyberspace in *Joint Publication 1-02*, as "the notional environment in which digitized information is communicated over computer networks."[66] This definition focuses mainly on the support or notional side of cyberspace and does not address the operational or physical aspects. For example, the DoD defines aerospace as pertaining to the "Earth's envelope of atmosphere and the space above it; two separate entities considered as a single realm for activity in launching, guidance, and control of vehicles that will travel in both

[65] Ibid, 4.

[66] "DoD Dictionary of Military Terms," DoD Dictionary of Military Terms, http://www.dtic.mil/doctrine/dod_dictionary/index.html (accessed November 18, 2009).

entities."[67] The latter definition addresses all aspects of aerospace operations while cyberspace operations are defined only in a support role. The DoD definition of aerospace covers the airfields needed for launch and recovery of aircraft, as opposed to the DoD definition of cyberspace where authors do not include the corresponding network switching hubs, network control centers and electromagnetic spectrum.

In the *National Military Strategy for Cyberspace Operations*, cyberspace is defined 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 infrastructures."[68] This was one of the first official definitions of cyberspace that expanded from just the hardwired Internet to include wireless aspects. In this definition, one can also see the inclusion of the associated physical structures needed to support cyberspace, paralleling the definition of aerospace outlined in the previous paragraph.

In 2008, Deputy Secretary of Defense Gordon England defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[69] Despite an increasingly comprehensive definition of cyberspace through the years, the publication of England's memorandum to all services marks a backwards trend with regard to the topic. England only defines cyberspace using a very limited Internet focus that addresses support infrastructure, but fails noticeably to include wireless aspects including data links covered under the electromagnetic spectrum.

---

[67] Ibid.

[68] *National Military Strategy for Cyberspace Operations* (Washington D.C.: Joint Chiefs of Staff, December 2006), IX.

[69] Gordon England, *The Definition of Cyberspace: Deputy SECDEF Memorandum to Secretaries of Military Departments* (May 12, 2008).

As is apparent, the definition of cyberspace is still in flux. Moving forward with the analysis, this monograph uses a combination of the last two definitions for cyberspace: *a global domain within the information environment consisting of the interdependent network of information technology, physical infrastructures, and the electromagnetic spectrum to store, modify, and exchange data via networked systems.* Unlike previous definitions of cyberspace, this definition covers the natural and artificial hardware aspects of cyberspace to include the data links between vehicles operating across the other domains (air, land, sea or space), the traditional Internet, the integrity and nature of data, and all information transport hubs.

Cyber War

The next topic that readers must understand involves the current definition and extent of cyber war. In his article *"The Cyber-defence Force's Virtual Shield,"* Robert West defined cyber war as "the use of computer intrusion techniques and other capabilities against an adversary's information based infrastructure to intentionally affect national security or to further operations against national security."[70] Currently, the DoD does not have a common definition for cyber war, but *Joint Publication, 3-13, Information Operations* defines computer network operations as "comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations."[71] With such a limited understanding of cyber war, U.S. officials may restrict cyber warfare to a defensive role, unlike West's definition that exhibits a more offensive spirit. Additionally, the current DoD definition of computer network operations remains incomplete. While the phrase cyber war implies multiple and synchronized actions

[70] Robert C. West, "The Cyber-defence Force's Virtual Shield," *Janes Intelligence Review* (December 2000): 17-18.

[71] *Joint Publication 3-13*, GL-6.

against an enemy, computer network operations implies limited and isolated actions primarily to protect information.

Computer Network Attack

To further explore the nature of computer network operations, *Joint Publication 3-13* defines computer network attacks as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[72] One classic example of a computer network operation is the cyber attack on Estonia in April 2007. In her article *Victory in Cyberspace,* Dr. Rebecca Grant described this event as Web War 1:

> Someone launched a massive, no-warning cyber. In its opening minutes, bursts of electronic messages began to flood Estonian government websites. Firewalls were up, extra servers were ready, and an emergency response team was standing by for just such an eventuality. Yet these defenses were easily breached. The attack count experienced exponential growth. There were about 1,000 assaults on the first day. On the second day, there were 2,000 attacks *per hour*. These denial-of-service attacks quickly forced the Estonian government to shut down several websites—some for hours, some for days.[73]

U.S. Secretary of the Air Force Michael Wynne also commented on the attack: "Russia, our Cold War nemesis, seems to have been the first to engage in cyber warfare . . . Over the past four weeks, it is reported that Russia has been conducting massive cyber attacks against the small Baltic country of Estonia – the first known incidents of such an assault on a state."[74] Thanks to Wynne's comments and other forewarnings from cyber officials, the United States and the world took notice and began to integrate cyber war into the planning process.

---

[72] *Joint Publication 3-13*, GL-5.

[73] Rebecca Grant, *Victory in Cyberspace*, Air Force Association Special Report (Arlington, VA: Air Force Association, October 2007), 4.

[74] TSgt A.J. Bosker, "SECAF: Dominance in cyberspace is not optional," *Air Force Print News*, May 2007.

According to draft U.S. Air Force cyber doctrine, computer network attack includes network attack, electronic attack, or physical attack. Network attack is an attack using network-based capability aimed to destroy, disrupt, or corrupt information resident in or transiting through networks.[75] Electronic attack is aimed at reducing the enemy's effective use of the electromagnetic spectrum (e.g. jamming).[76] Physical attack is a typical kinetic attack on known enemy cyber nodes to deny this capability.[77] A physical attack may also be used to shift an enemy's command and control communications onto a network that one already has compromised; for example, one may deliberately destroy an adversary's fiber optic network in order to deliberately force them to utilize instead significantly more vulnerable radio communications.

Computer Network Defense

The next definition critical to understanding the cyber domain involves both active and reactive defensive measures that nations must take to protect information, software, and systems. *Joint Publication 3-13* defines computer network defense as "actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks."[78] Computer network defense does not just apply to networks, but also to the physical and environmental pieces needed to execute cyberspace operations. Defensive activities typically have two major components: active and reactive. Active defenses are the continuous monitoring and analyzing of all activity and identifying anomalous behavior. Reactive defenses are the measures taken to

---

[75] *Air Force Doctrine Document 2-X: Cyberspace Operations (Draft)* (Washington D.C.: Department of the Air Force, 2009), 16.

[76] Ibid, 16.

[77] Ibid, 17.

[78] *Joint Publication 3-13*, GL-5.

directly counter adversary activities that seek to penetrate a network or actions taken to terminate an ongoing intrusion.[79]

Computer Network Exploitation

Finally, in addition to understanding both offensive and defensive cyber measures, readers must also understand computer network exploitation to better comprehend the intricacies of enabling such attacks. *Joint Publication 3-13* defines computer network exploitation as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[80] Computer network exploitation reveals information resident on or in transit through an adversary's system. Consequently, computer network exploitation can reveal vital information about an adversary's cyberspace and expose critical vulnerabilities. Additionally, computer network exploitation can generate vital strategic and operational intelligence for other operations including those executed across traditional domains like air, land, sea, and space.[81] Authors of recent articles on computer network exploitation typically address incidents within the DoD. For example, as late as 2009, U.S. Secretary of Defense Robert Gates admitted to a successful attack to steal highly sensitive, classified, and reportedly protected data involving the U.S. Air Force's F-35.[82] Beyond DoD, computer network exploitation can also apply to commercial industry. However, companies are not as quick to highlight that their systems were accessed and exploited since such an intrusion could potentially lead to loss of confidence in the company and have an irrevocable negative impact on stock prices or business opportunities.

---

[79] Air Force Doctrine Document 2-X: Cyberspace Operations (Draft), 14.
[80] *Joint Publication 3-13*, GL-6.
[81] Air Force Doctrine Document 2-X: Cyberspace Operations (Draft), 17.
[82] Gates: Cyber Attacks a Constant Threat, *CBS News*, April 21, 2009. http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml (accessed January 14, 2010).

Computer network attack, computer network defense and computer network exploitation are three aspects of computer network operations and taken collectively, provide the reader with an understanding of DoD's existing conception of cyber war. However, to ascertain a more complete definition of cyber war one must understand more than just the different types of attacks and defensive measures and explore the nature, intent, and source of such attacks. Due to the amorphous structure of the cyber domain, both state and non-state actors can operate across cyberspace. As a result, to fully understand cyber war readers must learn the subtle distinctions between cyber crime, cyber terrorism, and hacktivism.

Cyber Crime

The *2006 QDR* tasked DoD to be able to effectively shape and defend its cyber networks.[83] To meet this task, the DoD needed to understand what constitutes cyber crime. In her monograph *The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?,* Major Bonnie Adkins defined cyber crime as activity which "ranges from illegal exploration, hacking or other computer intrusions perpetrated by an individual or group with criminal or self-motivated interests and intent."[84]

Cyber crime can include theft of technology, information, or both in the form either of a criminal act or as an act of espionage, which significantly complicates the problem. For example, in a criminal act the Department of Justice (DoJ) would be the lead agency retaining both investigatory and prosecution responsibilities. However, in an espionage case directed against the United States, either DHS or the DoD would be responsible.[85] In 2009, hackers stole $300 billion in F-35 fighter development proprietary technology. According to Secretary of Defense Gates, the

---

[83] *Quadrennial Defense Review 2006*, 31.

[84] Bonnie Adkins, *"The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcements Role?*" (master's thesis, Air Command and Staff College, Air University, April 2001).

[85] *National Strategy to Secure Cyberspace*.

breaches took place in the allied nation of Turkey. [86] Although the attackers certainly had malicious intent, the individuals were more than likely acting with financial, not ideological or political motivation. Regardless, as the example indicates, the United States needs to focus its efforts on providing a flexible cyber force that can meet a wide range of threats, not just from known or suspected terrorists.

Cyber Terrorism

Major Adkins further defined cyber terrorism as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data, which result in violence against noncombatant targets by sub-national groups or clandestine agents."[87] Unlike cyber crime related attacks, the actions of cyber terrorists are inspired by more than just financial motivations. The 2007 attack against Estonia was initially classified as a cyber terrorist attack. Complicating efforts to define the nature of the attack, Russia denied any responsibility for the measures and pointed out that it was a concerted effort of hackers functioning in a supposedly unsponsored fashion.[88]

One of the biggest concerns of U.S. officials is an attack by cyber terrorists on U.S. critical infrastructure such as the electrical grid or telecommunication network. A report by the Congressional Research Service highlighted a potential scenario referred to appropriately as the "Digital Pearl Harbor":

> In July 2002, the U.S. Naval War College hosted a war game called "Digital Pearl Harbor" to develop a scenario for a coordinated cyber terrorism event, where mock attacks by computer security experts against critical infrastructure systems simulated state-sponsored cyber war. The simulated cyber attacks determined that the most vulnerable infrastructure computer systems were the Internet itself, and the computer

---

[86] Gates: Cyber Attacks a Constant Threat, *CBS News*, April 21, 2009. http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml (accessed January 14, 2010).

[87] Adkins, 26.

[88] Grant, 5.

> systems that are part of the financial infrastructure. It was also determined that attempts to cripple the U.S. telecommunications infrastructure would be unsuccessful because built-in system redundancy would prevent damage from becoming too widespread. The conclusion of the exercise was that a "Digital Pearl Harbor" in the United States was only a slight possibility.[89]

As technology flourishes globally and access to this technology increases, the threat of attacks by cyber terrorists will only increase. As a result, it behooves the U.S. and its allies to take protective measures.

Hacktivism

An introduction to hacktivism, another grey area between criminal activity and terrorist attacks, will more fully contribute to an overall understanding of cyber war. Hacktivism is defined as "computer activism and operates in the tradition of non-violent direct action and civil disobedience."[90] Hacktivism uses the same tactics of trespass and blockade from earlier social movements and applies them to the Internet. This type of operation occurs as a denial of service during certain politically controversial events.[91] One of the most recent examples of hacktivism is hacking into the Climatic Research Unit of the University of East Anglia in Britain. Anti-global warming hacktivists were able to steal emails and post them to the Internet as evidence that scientists rigged data to make it appear as if humans caused global warming.[92]

This chapter has explored the nature of cyber war in depth. In addition to more fully defining the cyber domain and operations, this section has described the multiple facets of cyber war. Readers should now understand that cyber war includes more than just the DoD offensive and defensive functions, but also includes both criminal and terrorist aspects which blur the line

---

[89] Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Washington D.C.: Congressional Research Service, January 29 2009), 20.

[90] Adkins, 8.

[91] Juliet Eilperin, "Hackers steal electronic data from top climate research center," *Washington Post*, November 21, 2009.

[92] Ibid.

between military operations and law enforcement. As cyber doctrine matures and is more clearly defined, government officials and military personnel will better understand how to apply cyber capabilities. Now, with an understanding of both the Principles or War and cyber war, this paper endeavors in the following chapter to address the primary research question of whether or not the Principles of War apply to cyber war.

Do the Principles of War Apply to Cyber War?

> The advent of cyber warfare, which can go straight to the vital centers and either neutralize or destroy them, has put a completely new complexion on the old systems of making war. It is now realized that the hostile main army in the field is a false objective, and the real objectives are the vital centers.
>
> John Osterholz[93]

With the advent of airpower, officials had similar discussions as the current debate over cyber war and the Principles of War. In the epigraph above, John Osterholz took a quote from Brigadier General Billy Mitchell regarding airpower and replaced air warfare with cyber warfare to show to striking similarities. Like Mitchell advocating the capacity of airpower years earlier, Osterholz questioned why the United States should ever risk attacking with physical assets when an attack with cyber capabilities can produce similar results. As discussed earlier, contemporary U.S. leaders have relegated cyber related activities to primarily a support role rather than an active or direct tool. Similarly, when Brigadier General Mitchell advocated the use of airpower to achieve national objectives, critics questioned whether airpower could do anything besides provide support. Just as Mitchell argued for a more appropriate application of airpower, this monograph attempts to encourage a similar discussion that challenges U.S. civilian and military leaders' notion of conventional conflicts with regard to the cyber domain.

As General of the Army MacArthur quipped, "New conditions require, for solution–and new weapons require, for maximum application–new and imaginative methods. Wars are never won in the past."[94] MacArthur highlighted that one must not live on successes of the past or within traditional paradigms when confronted with revolutions in military affairs. At the same time, one cannot discount the past and must strive to glean lessons from history's successes and

---

[93] John Osterholz, "Data Bombs Away," *Armed Forces Journal* (September 2009).
[94] Westenhoff, *The CADRE Digest of Air Power Opinions and Policy Issues*, 56.

failures that apply in a contemporary context. As airpower in the past, cyber power today represents a new application of military technology that some initially argued brought a revolution in military affairs; also like airpower in the past, cyber power has instead turned out to be a military revolution that will continue to have far-reaching impacts for both military and civilian sectors alike.

The remainder of this chapter compares the Principles of War from chapter two with the cyber definitions from chapter three. This comparison shows where cyber fits within the current and generally accepted understanding of the Principles of War and highlights particular areas where the existing paradigm proves insufficient.

Objective

The purpose of the objective is to direct every military operation toward a clearly defined, decisive, and achievable goal.[95] With cyber operations, planners need to integrate computer network operations into the stated objective of the joint force commander. Leveraging the ability of the cyber domain, offensive cyber operations can enable strategic, operational, and tactical effects through functional missions such as strategic attack, counterair, counterland, countersea and space control.

Depending on the objective of the joint force commander, a cyber effort may either involve either attack or defense. For example, an objective may be to disrupt an enemy's command and control through a cyber attack directed against a power grid. Through computer network attack, a joint force commander can disable a power grid without using kinetic weapons. As a result, the joint force commander does not need to take into consideration the need to rebuild the power infrastructure during post-conflict operations. By including cyber capabilities in such a

[95] *Joint Publication 3-0*, A-1.

direct role, equal to a conventional bombing campaign against the same target, a joint force commander can significantly reduce the amount of time required to bring about stability and meet the national strategic objectives identified by the President. Additionally, by minimizing the amount of time and forces required to stabilize an area of operations, leaders can drastically increase the combat power available for other issues that a commander may face to ensure that the right forces are applied towards the objective.

In his book, *The Principles of War for the Information Age*, Robert Leonhard argued that the principle of objective does not apply to cyber war. Leonhard contended that the principle of objective focuses military forces on the decisive battle.[96] Furthermore, since the nature of cyber war is inherently continuous and it is often difficult to identify a clear and decisive virtual "battle," Leonhard contended that objective, as traditionally defined, does not apply to the cyber domain. Despite Leonhard's contention, commanders do nevertheless need to identify a clear objective to focus all efforts to include cyber operations. Leonhard focused on the tactical level of battle and consequently failed to consider the principle at the strategic level of war and the effect desired. In fact, joint force commanders are guided by the principle of objective at the higher echelons of war. Without an objective to focus the actions of joint forces, how do subordinate commanders know when they have reached termination criteria? Strategic level objectives should be based on the termination criteria that the commander or higher civilian authority has published. Therefore, once the appropriate officials have established such objectives, military officials must then strive to incorporate how, and to what extent, cyber related activities could best achieve the desired effects. Contrary to Leonhard's remarks, the decisive battle in today's world could very well focus the joint force on an objective that is appropriately accomplished through cyber operations.

---

[96] Leonhard, *The Principles of War for the Information Age,* 141.

Offensive

The purpose of an offensive action is to seize, retain, and exploit the initiative.[97] Although a traditional understanding of this principle may indicate that initiative involves seizing terrain, a more contemporary understanding significantly broadens the definition. Just as airpower seizes, retains and exploits the initiative in the air domain, cyber can seize, retain, and exploit the initiative in the cyber domain. As an example of a cyber offensive, consider the computer network attack on behalf of supposedly non-state actors in Russia against the state of Estonia described in chapter three. The offensive in cyber war may include a network, electronic warfare or a physical attack to seize the domain for exploitation and follow-on operations.

Similarly, during the 2008 incursion into Georgia by Russian military forces, cyber forces conducted an offensive against the Georgian military and government. Russian forces conducted a full-spectrum offensive to deny the use of radio waves as well as to prevent the use of the Internet within the country of Georgia. As a result, the Russian cyber offensive blinded the Georgian military and reduced drastically their command and control capacity.[98]

In his book *The Principles of War for the Information Age*, Leonhard again disagreed with the validity of the principle of offensive in the information age. Since the definition of offensive, according to Leonhard, does not address the defensive responsibilities of military forces, the principle does not adequately cover cyber efforts.[99] If one analyzes the nature of cyber conflict with respect to the principle of offensive in isolation from all the other precepts, then Leonhard may have a valid contention. However, the author fails to consider that defensive responsibilities are covered extensively through other principles such as security. Clausewitz highlighted in his book *On War* that "If the enemy is to be coerced you must put him in a

---

[97] *Joint Publication 3-0*, A-1.
[98] Tom Espiner, "Georgia accuses Russia of coordinated cyberattack," *CNET*, 11 August 2008.
[99] Leonhard, 82.

situation that is even more unpleasant than the sacrifice you call on him to make."[100] In other words, a commander may not be able to inflict sufficient consequences on an enemy if his forces remain in the defensive mode. Only through offensive action can a commander compel an enemy to comply with a commander's intentions. An attack, with exclusively cyber forces, can retain an offensive nature that potentially convinces an enemy to face a more desirable situation than any alternative.

Mass

The purpose of mass is to concentrate the effects of combat power at the most advantageous place and time to produce decisive results.[101] Just as in a kinetic fight, it is necessary to concentrate cyber firepower at the right place and time for decisive results. A joint force commander can mass electronic warfare packages on the right location to blind an enemy, to force movement, or to provide security. A military force can also conduct a cyber network attack to deny an enemy satellite communications or telephone infrastructure.

Like ammunition or airframes, the cyber capacity of a force is still limited in both scope and application. Since the U.S. military has a finite amount of cyber capabilities, the joint force commander must prioritize where and when to mass forces and intended effects to complete a given mission. With the stand up of United States Cyber Command, the joint force commander will be better able to gain access to the full cyber capabilities of the U.S. military without having to deal with the bureaucratic requirements of each of the individual services. [102] Regardless of resource challenges, even using the most traditional definition of the principle of war, the principle of mass clearly applies to the cyber domain.

---

[100] Clausewitz, *On War*, 77.
[101] *Joint Publication 3-0*, A-1.
[102] Donna Miles, "Gates Establishes New Cyber Subcommand," *American Forces Press Service* (June 24 2009).

However, Leonhard again disagreed and equated mass exclusively with boots on the ground, i.e. mass can only equal the number of available personnel.[103] In his limited definition, however, Leonhard does not address the concept of massing effects. In modern warfare, the concept of mass also applies to the effect that a joint force commander seeks and not just the forces available. A commander weighs how best to achieve an effect and then determines the method of massing to gain that effect. A modern commander considers his approach across all domains including air, land, sea, space and cyber to decide which domain he wants to engage the enemy through the application of mass. For example, a commander may choose to mass effects through multiple domains simultaneously such as a concurrent cyber network attack and a kinetic air strike to disrupt an enemy commander's command and control capacity. Based on this expanded and commonly accepted definition of mass, one can refute Leonhard's contention; the principle of mass absolutely applies in the cyber domain as much as or more than the traditional domains.

Economy of Force

The purpose of economy of force is to allocate minimum essential combat power to secondary efforts.[104] Supporting this traditional definition, Clausewitz pointed out the need "to make sure that all forces are involved" in any military endeavor. [105] However, just as there are only so many kinetic forces for use, there are also only so many cyber capabilities within the U.S. military. A joint force commander needs to prioritize the most efficient use of his force for the desired effect. The joint force commander can choose to destroy a target with either kinetic or non-kinetic means. If the joint force commander uses a cyber capability to achieve an effect, he

---

[103] Leonhard, 115.
[104] *Joint Publication 3-0*, A-2.
[105] Clausewitz, *On War*, 213.

can then free up additional combat power for another mission. Especially on the modern battlefield, one can understand how the joint force commander may want to accomplish more with a limited force and preserve other assets for requirements that can only be accomplished in a more traditional manner. In light of such an analysis, the reader can begin to understand how the concept of economy of force invariably applies to the cyber arena.

Despite his predominantly critical outlook on the Principles of War applying within the cyber domain, even Leonhard agreed with the notion that cyber efforts definitely support an economy of force approach. Leonhard appropriately indicated that there are only so many forces available and some are not replaceable. Therefore, using a cyber asset in lieu of an indispensable one makes complete sense. Leonhard also noted that the principle of economy of force has economic implications for a nation with limited financial support for its military's actions.[106] Therefore, since a cyber effort can potentially save financial resources in accomplishing a mission in place of traditional firepower, one can further witness how this long-standing principle of war still applies to the cyber domain.

Maneuver

The purpose of maneuver is to place the enemy in a position of disadvantage through the flexible application of combat power.[107] In this sense, the long reach and the rapid flexibility of cyber assets are especially noteworthy. However, the challenge of maneuver in the conduct of cyber operations is that the cyber environment is constantly changing and the enemy often possesses similar advantages. Portions of cyberspace change due to technical adjustments including the addition, removal, replacement, or reconfiguration of components or networking protocols. U.S. military and civilians must understand that maneuver paths available in the past

---

[106] Leonhard, 124.
[107] *Joint Publication 3-0,* A-2.

might not be available for exploitation in the future. For example, in January of 2009, an underground fiber cable was cut off Egypt isolating the country and significantly reducing Internet access to the Middle East and India.[108] Just like ground forces moving up a road to find a bridge is out or the road mined, a cut cable makes a cyber avenue unavailable. Consequently, with the loss of the physical structure, any cyber efforts tied to that cable were also lost. Like a destroyed bridge negatively influencing the maneuver capacity of a ground force, the destroyed cable negatively affected the virtual maneuver capacity of cyber actors.

Leonhard proposed that maneuver is an outdated principle in the context of the cyber arena.[109] However, he focused on the physical aspects of the principle and did not fully realize the maneuver potential available to commanders in today's globally connected world. When Leonhard wrote his book in 2000, the world was not as connected as it is today. Cyber was just coming forward conceptually and the Internet boom that occurred in the first ten years of the 21st century had yet to occur. Through globalization, the Internet offers a maneuver capability that is logical versus physical.

With information growing in an exponential fashion, the benefits and downsides of cyber maneuver are also increasing. Expanded connectivity, facilitates the conduct of cyber warfare by all entities, both good and bad. In 2009, 25 percent of the world's population (1.7 billion) used the Internet.[110] Consequently, the United States can theoretically conduct cyber operations in terrain that remains inaccessible to air, land or sea forces due to traditional defenses in depth. Cyber operations open up new ways of putting the enemy at a disadvantage before the first kinetic shot. For example, consider the middle-aged Iranian "twittering" the atrocities conducted

---

[108] Camilla Hall, "Mediterranean Cables Cut, Disrupting Communications," *Bloomberg*, 2008. www.bloomberg.com.

[109] Leonhard, 53.

[110] "Internet Usage Statistics," Internet Usage Statistics, http://www.internetworldstats.com/stats.htm (accessed March 15, 2010).

by the Iranian leadership after the 2009 election.[111] Completing a feat that might not have been possible in the past, non-state actors exploited maneuver room within the cyber domain, conducted cyber operations to expose the democratic weaknesses of the nation-state, and ultimately transmitted a message out of a country that supposedly restricted Internet access. Because of this information, other nations were then able to diplomatically pressure Iranian leadership, letting them know that the world not only disapproved of the conduct of the elections, but was also watching carefully how they handled the situation. In this expanded, yet strikingly similar, definition of maneuver, a reader can certainly understand how this Principle of War applies to the cyber domain.

Unity of Command

By its doctrinal definition, unity of command is currently out of alignment with respect to the conduct and management of cyber forces operating in the cyber domain.[112] Within the joint arena, there is no publication on command and control of cyber operations. *Joint Publication 3-30 Command and Control for Joint Air Operations*,[113] *Joint Publication 3-31 Command and Control for Joint Land Operations*[114] and *Joint Publication 3-32 Command and Control for Joint Maritime Operations*[115] all provide joint guidance for the other three domains. Authors of these documents outline clearly the foundations for command and control relationships for each of the land, air, and maritime functional component commanders. However, none of these joint publications specifically states which functional component commander has overarching control

[111] Twitter Links Iran Protesters to Outside World, *Fox News*, June 16, 2009.

[112] Donna Miles, "Gates Establishes New Cyber Subcommand," *American Forces Press Service* (June 24 2009).

[113] *Joint Publication 3-30 Command and Control for Joint Air Operations* (Washington D.C.: Joint Chiefs of Staff, January 12, 2010).

[114] *Joint Publication 3-31 Command and Control for Joint Land Operations* (Washington D.C.: Joint Chiefs of Staff, March 23, 2004).

[115] *Joint Publication 3-32 Command and Control for Joint Maritime Operations: Incorporating Change 1 27 May 2008* (Washington D.C.: Joint Chiefs of Staff, August 8, 2006).

of space and cyber forces. Command and control of each warfighting capability is critical. Similarly, command and control of cyber related activities must be assigned to a single organization to avoid severely disjointed efforts on behalf of joint forces and to decisively establish unity of command within the operational environment.

Within DoD, the Secretary of Defense has directed that all cyber units and operations fall under the new Unified Functional Combatant Command called United States Cyber Command (USCYBERCOM).[116] United States Cyber Command is a sub-unified command under United States Strategic Command (USSTRATCOM), which has responsibility for the computer network operations mission as tasked under the Unified Command Plan.[117] Such a reorganization effort will invariably streamline all cyber operations under one commander. Currently, each of the military services develops their own cyber capabilities, which work in isolation and are not coordinated with the other services. However, although the new USCYBERCOM will reach full operational capacity in October of 2010, the services will still control funding and organizational responsibilities associated with the new organization. Although most recognize the necessity to exhibit unity of command in the cyber domain, only service cooperation in the future will make this critical Principle of War fully applicable in a cyber context. The United States government has charged DHS as the responsible agency for ensuring the security of the nation's infrastructure.[118] Despite elements of cyber terrorism, cyber espionage and a general cyber war directed against the United States, coordination between DHS and DoD is not as robust as the relationship between DHS and law enforcement agencies. Adding to an already disparate relationship with respect to unity of command, current intelligence oversight laws hinder the use

---

[116] Donna Miles, "Gates Establishes New Cyber Subcommand," *American Forces Press Service* (June 24 2009).

[117] *Unified Command Plan 2008* (Washington D.C.: Secretary of Defense, 2008).

[118] *National Strategy to Secure Cyberspace*.

of DoD cyber assets to augment DHS for homeland defense or the Department of Justice for counter-cyber criminal activities. These laws contribute even further to a disjointed unity of command in applying the cyber capacity of the whole-of-government.

In his book, Leonhard argued that unity of command is another outdated principle with respect to the cyber domain. Leonhard highlighted that U.S. military forces have become too big for one commander to command and control. [119] However, without a single commander designated to provide unity of command, military forces and efforts will be wasted. A cursory analysis of the Desert One scenario in the Iran hostage rescue provides a great example of what can happen without unity of command. To learn lessons from Desert One, DoD charged Admiral James Holloway with creating an assessment of events which not only contributed to what would become known as the "Holloway Report" but also led to the Goldwater-Nichols Act that restructured the military in 1986. Using the Holloway report as a guide for analysis of Desert One, one can see that the forces involved did not know who had what authority, especially the authority to rescind the mission based on collective observations of events on the ground.[120] Unity of command under a single commander would have solved this problem according to Admiral Holloway's assessment.

Desert One highlighted the need for unity of command. As U.S. forces have increased in size, the U.S. military has also introduced technological advances to provide adequate capability for commanders to maintain control commensurate with the sizes of their forces. New command and control systems allow the commander to direct forces in contact and even watch the battle occur with live streaming video. Some may contend that these types of control mechanisms have introduced a vulnerability for U.S. forces by allowing the enemy an opportunity to attack critical

---

[119] Leonhard, 194.

[120] Admiral James Holloway, *Special Operations Review Group: Iran Hostage Rescue* (Washington D.C.: Joint Chiefs of Staff, August 23, 1980), 50.

technological assets. Cyber capabilities need to simply be more robust in ensuring that these command and control tools remain available to commanders. Contrary to Leonhard's premise that the concept of unity of command is outdated due the increasing size of U.S. forces in a cyber context, operating in such an environment actually increases the demand for unity of command. Furthermore, with increasingly large force developments within the cyber domain have made it possible to improve command and control as well. USCYBERCOM, as a functional component command, will provide not only the necessary forces but also the requisite structure to ensure that command and control is maintained by and for friendly forces. Such efforts are a testament to the validity of the unity of command principle in a cyber context.

Security

The purpose of security is to never allow the enemy to acquire an unexpected advantage.[121] In the context of the cyber domain, this enduring principle of war still has tremendous value. The typical cyber capability associated with security is computer network defense. The cyber community must continuously challenge the level of connectivity to different networks both internally and externally. A joint force commander must weigh the mission impact of a computer network attack on U.S. forces and constantly determine what can be isolated with the least negative effect.

Encryption over a network, or even on radios, is one means of conducting basic security measures. Cyber military forces need to ensure that they are up to date on the latest encryption, yet at the same time minimize operational impacts of the encryption of various devices throughout the force. Loading software to fix a non-mission critical vulnerability during an operation might have negative impacts. Providing blanket blockage of websites can hinder

[121] *Joint Publication 3-0*, A-2.

contract operations critical to mission support success. Cyber defense operations personnel need to weigh these requirements and understand that making a network 100% secure may mean making a mission unachievable.

Another computer network defense capability is self-imposed degradation. If an enemy is exploiting friendly cyber capabilities for their own operations, friendly forces can degrade or isolate the capability the enemy is using. One potential scenario would be to degrade the Global Positioning System (GPS) satellite constellation so that only United States military could get its full capabilities. However, the higher order effects of such a decision would be virtually endless. A commander would have to consider first the impact on coalition forces operating outside the area of operations. Additionally, the commander would have to weigh the impact on neighboring countries dependent on such a system. If the GPS constellation was intentionally degraded by U.S. forces without appropriate coordination beforehand or the appropriate strategic communication message afterwards, such an action could potentially alienate neutral countries or, worse yet, encourage them to support an opponent.

To ensure continued cyber security, cyber forces need to maintain constant vigilance of the cyber domain for potential threats. U.S. officials must take such security measures to prevent the cyber Pearl Harbor from happening to the nation. U.S. cyber entities have already caught Russian and Chinese cyber espionage forces conducting reconnaissance of the U.S. electrical power grid.[122] With such data in the hands of an adversary, the enemies of the United States could easily conduct directed cyber network attacks on the electrical power grid that would result in the destruction of power generation capabilities. The Department of Energy conducted an exercise in which officials successfully destroyed a generator through computer commands. By exploiting

[122] Spies Penetrate U.S. Electrical Grid: National Security Officials Say System Is Under Attack From Russian And Chinese Cyber Spies, *CBS News,* April 2009. http://www.cbsnews.com (accessed March, 2010).

automation that has put virtual control systems in place to reduce the work force's requirement for power production, Sandia Laboratory successfully forced a generator to self-destruct by remotely pushing the generator out of its normal operating tolerances. Generators such as this are expensive and can take up to six months to replace.[123] If a state or non-state actors could successfully target the U.S. energy infrastructure using the type of information countries have already sought to acquire, one can expect that paralysis of the nation would result.

Security is especially critical and valid in a cyber context. The previous analysis highlighted just a few publicly accessible examples of what can happen if an opponent is successful in conducting cyber operations against the United States. One of the first tasks of USCYBERCOM is to consolidate all DoD cyber security capabilities in order to eliminate potential vulnerabilities that a service might have. This will ensure that U.S. cyber capacity is secure and available to the force when needed for combat operations.

Surprise

In his book *Principles of War*, Clausewitz emphasized the principle of surprise, stating that it "plays a much greater role in strategy than in tactics. It is the most important element of victory. Napoleon, Frederick II, Gustavus Adolphus, Caesar, Hannibal, and Alexander owe the brightest rays of their fame to their swiftness."[124]

Accordingly, the purpose of surprise is to strike at a time, place, or in a manner for which the enemy is unprepared.[125] The U.S. cyber forces need to maintain freedom of maneuver to be able to conduct a surprise cyber operation where and when least expected. This could include a

---

[123] *Cyber Effects: Analysis using VCSE* (Sandia National Laboratories, September 2008).
[124] Clausewitz, *The Principles of War*.
[125] *Joint Publication 3-0*, A-3.

computer network attack in which friendly cyber elements destroy a country's command and control capability through a quick cyber response, such as a first strike.

In April of 2007, Russia achieved surprise in the cyber domain against the country of Estonia. The former Soviet bloc country was not prepared for the severity of the attack. Although Russian efforts did not completely cripple Estonia, the disruption of services affected every citizen, sending a very clear message to the Estonian people from their former Russian masters. As the first documented cyber attack against a nation, the Russians not only surprised Estonia but also NATO and the United States who realized, upon analysis, that their military forces needed to be able to counter a similar computer network attack.[126] In response, NATO stood up the Cyber Warfare Center of Excellence to train NATO forces on cyber warfare within Estonia. As the Estonian government can certainly attest, the principle of surprise, with origins as far back as Sun Tzu and beyond, remains especially relevant when considered in the context of the modern cyber domain.

Simplicity

The purpose of simplicity is to prepare clear, uncomplicated plans and concise orders to ensure thorough understanding throughout the chain of command.[127] Like the employment of any kinetic force, any employment of cyber forces needs to be as simple as possible. In addressing the idea of friction, Clausewitz began with "Everything in war is simple, but the simplest thing is difficult."[128] He then defined friction as "the force that makes the apparently easy so difficult." Clausewitz expanded on his explanation of friction using a metaphor of fog, which represented the uncertainty that shrouds any battlefield. A good commander wants to eliminate friction or

---

[126] William Ashmore, "Impact of Alleged Russian Cyber Attacks" (master's thesis, School of Advanced Military Studies, 2009), 4.

[127] *Joint Publication 3-0*, A-3.

[128] Clausewitz, *On War*, 119.

"fog" in order to "see" to take advantage of any opportunity that might occur. By developing and adhering to a simple plan, the joint force can reduce Clausewitz's proverbial fog and see the complex battlefield more clearly.

Since the cyber domain crosses all traditional domains including air, land, sea, and space, aspects of the cyber domain may be more difficult to control and monitor. However, by keeping the conduct of cyber operations simple, one can help reduce potential elements of friction that inevitably occur as the best laid plan comes into contact with reality; a simple cyber operation integrated into a joint force commander's larger operation can help achieve desired results.

Robert Leonhard argued that the principle of simplicity is again outdated in a cyber context; according to Leonhard, simplicity is impossible since modern military conflicts involve large forces, which only increases complexity rather than reduces it.[129] Although Leonhard's basic premise may have elements of the truth, his logic assumes that only a complex plan will work in a complex environment. Although large forces may certainly increase the complexity of a given situation, this truth does not invalidate the utility of simplicity, especially in planning large operations. Even a large military force can benefit from a simple plan that makes it easier for the subordinate commander to focus forces on a given objective. Complex plans on the other hand have the potential to create confusion on the battlefield. Leonhard's contention does not detract from the fact that the appropriate application of the principle of simplicity can still have resounding positive results in the cyber domain.

[129] Leonhard, 170.

Restraint

The purpose of restraint is to limit collateral damage and prevent the unnecessary use of force.[130] Just as other military operations organized in space and time to maximize their effect, a joint force commander must balance force exerted to defend a cyber network with force applied to achieve other objectives. If the commander places too much emphasis on computer network defense, he may risk collateral interference of other missions, such as logistical supporting efforts. In many existing networks, one communications link may provide both secure and non-secure voice and data transmission capabilities. However, if a friendly element disconnects the link in an effort to provide computer network defense, one might inadvertently disable an isolated unit's sole secure link to both higher headquarters and subordinate units.

A joint force commander needs to judiciously exercise restraint when deciding the extent and nature of any computer network attack. The U.S. military uses many of the same communications networks and nodes used by potential enemies. For example, if U.S. forces use a commercial satellite orbiting over a recently invaded country, the U.S. military may lease bandwidth on that satellite from a third party; however, potential adversaries may also be using bandwidth on the same satellite. By conducting a computer network attack on the satellite in an effort to secure data, a commander might jeopardize the operational capability of friendly forces as well. In a similar sense, commercial phone switches and Internet service providers are two other examples of common use hardware potentially employed by both friendly and enemy forces.

Finally, a joint force commander may want to exercise restraint in the cyber domain as knowing what the enemy is doing is often worth more than denying the enemy a capability outright. If an adversary was using a particular command and control asset that friendly cyber

[130] *Joint Publication 3-0,* A-3.

assets can deny or destroy, perhaps a better course of action would be to exercise restraint in order to gain intelligence. Additionally, if friendly intelligence has cracked the security protecting the enemy's communications node, by allowing friendly cyber forces to monitor the enemy's command and control, the joint force can extract an even greater benefit as they know what their enemy is doing. Just as in the application of kinetic weapons, the joint force commander needs to apply considerable restraint when deciding how best to employ cyber capabilities. Therefore, the concept of restraint as a principle of war has valid contemporary applications in the cyber domain.

Perseverance

The purpose of perseverance is to ensure the joint force demonstrates the appropriate level of commitment necessary to attain the national strategic end state.[131] In *On War*, Clausewitz highlighted the need for perseverance, writing "even the ultimate outcome of a war is not to be regarded always as the final one." [132] Clausewitz warned that, without perseverance, a commander might prematurely react to incomplete reports and haphazardly engage an enemy that exhibits either more or less capability than expected. [133] Colin Gray warned that Americans, given their aversion to casualties, might lose their perseverance if they experience what they deem to be excessive losses. [134] Regardless of the subtle differences among definitions, perseverance applies to the cyber domain in two respects.

First, in today's state of continuous conflict, friendly cyber forces need to stay ahead of the enemy's decision cycle. Since time is a precious asset for a cyber criminal or terrorist, the joint force must always "maneuver" assets to protect the force. To accomplish this formidable

---

[131] *Joint Publication 3-0*, A-4.
[132] Clausewitz, *On War*, 644.
[133] Ibid, 193.
[134] Colin S. Gray, *The American Way of War* (Reading: University of Reading, 2005).

task, friendly cyber forces have to continuously strive to update, change, and strengthen defenses, while iteratively seeking new methods of attack. To persevere, military cyber forces need to maintain the technological edge obtained through in-depth knowledge of foreign and domestic networks. Cyber forces need the flexibility to operate in multiple networks simultaneously, being able to relocate operations to a different network should one becomes unavailable. As both friendly and enemy forces conduct opposing offensive and defensive maneuvers, a cyber warrior has to retain the requisite perseverance to stay one-step ahead of the adversary.

Second, unlike in the past, the notion of perseverance in a cyber context represents perhaps the easiest and cheapest means to achieve objectives that would have traditionally required ground forces. Although deriving their operational capacity from within the continental United States, cyber forces can maintain a continuous presence globally with a minimized footprint at any location. It is significantly easier to persevere over a longer period with less resources in the cyber domain than in the other physical domains. Perseverance as a principle of war is not only still applicable to the cyber domain but also even more relevant than in the past.

Legitimacy

The purpose of legitimacy is to develop and maintain the will and image necessary to attain the national strategic end state.[135] The legitimacy of an operation is based on the legality, morality, and rightness of the actions undertaken. Just like kinetic operations, cyber operations must be viewed as legitimate in the eyes of both the cyber community and the impacted population. First, actions and responses within the cyber domain must be in proportion to each other to be deemed legitimate. For example, responding to a non-state actor committing cyber criminal activity by conducting an in-depth cyber attack that disables a region's power grid may

[135] *Joint Publication 3-0,* A-4.

not be viewed as a proportional, and therefore an illegitimate response. However, blocking a non-state actor's attempt to steal data, then cooperating with his home government to prosecute him under the nation's internal laws would be perceived as fair, just, and legitimate.

With respect to the cyber domain, U.S. intelligence oversight laws prevent illegal collection methods while protecting the populace from dangerous intrusions or attacks. By carefully balancing the requirements for national defense with legal obligations, the U.S. cyber force can retain the highest levels of legitimacy. As criminal prosecutions of cyber related violations occur, properly collected evidence gives legitimacy to both the legal system as well as the cyber force.

Legitimacy extends beyond legitimate collection and monitoring techniques, to targeting as well. If a commander decides to use cyber techniques to accomplish an objective, then the actions conducted by the cyber force need to be legitimate. If cyber operations direct efforts against traditional non-military targets like the Red Cross, or against non-state actors within clearly defined state boundaries, then the United States could face legitimacy issues that might adversely affect U.S. interests.

The notion of legitimacy is particularly difficult in the cyber domain since data collection or exploitation in not as clear-cut as unnecessary use of conventional force or human rights violations. Unlike the traditional domains with more defined rules of engagement, the cyber domain exists in a virtual world that defies precise definition. Nonetheless, without question legitimacy as a Principle of War applies to the cyber domain and is perhaps even more critical then with conventional operations.

SUMMARY

> "While it has been more than 55 years since the last American service member came under attack by enemy air-to-surface fires … the last time an American service member came under cyber attack was the beginning of this sentence."
>
> Secretary of the Air Force Michael B. Donley[136]

The Principles of War not only apply to the cyber domain, but also lend insight into the very nature of cyber war. Cyber brings new operational capabilities that joint force commanders can leverage to achieve mission success. To better integrate cyber into their operations, joint force commanders need a better understanding of these capabilities and their limitations.

This monograph has described the Principles of War and shown how these concepts developed over time. The Principles of War have proven resilient enough to survive through history but their perceived meaning depends upon their historical context. Just as the original nine Principles of War have helped shape the U.S. military for success through the 20th century, these same principles should stay as the foundation for military operations into the 21st century. The joint force must not, however, limit their application to the traditional understanding of these principles. The joint force commander must continually rediscover and reapply the essential truths of the Principles of War. By considering the principles on the virtual battlefield, U.S. military and civilian personnel can extract the same insight and meaning responsible for the durability of the principles over the years.

In the epigraph above, Secretary Donley highlighted the critical need for discussions concerning cyber war. The threat posed by cyber operations to the security of the United States requires the joint community to develop a force that no longer considers cyber as a support function, but recognizes the direct operational potential of the nation's cyber force. Current U.S.

---

[136] TSgt Amaani Lyle, "SecAF Delivers 'State of the Air Force' speech at AFA," *Secretary of the Air Force Public Affairs*, September 14, 2009.

strategic documents identify cyberspace as an operating domain equivalent to the air, land, sea and space domains. A review of current joint doctrine has shown that the joint community needs to further develop cyber operations. The U.S. military needs to standardize terminology within cyber operations through the publication of a separate joint publication series for cyber operations. With the activation of USCYBERCOM, the United States will gain an advocate within DoD to further the development and integration of joint doctrine for cyber operations.

Additionally, with USCYBERCOM the U.S. military has taken the first step toward defending national interests through the consolidation of all DoD cyber assets under one commander. This brings about the unity of command necessary to ensure the standardization of cyber forces. The next step for USCYBERCOM is to document the command and control relationship cyber forces will have with other traditional combatant commands. Just as *Joint Publication 3-30 Command and Control for Joint Air Operations* defines the command and control responsibilities for the air domain, the creation of an equivalent cyber publication will define similar authority. Taking such deliberate actions to codify the cyber domain will eliminate the confusion that exists about who has the command and control of cyber forces at the functional component commander level (e.g. JFACC, JFMCC, and JFLCC).

The Principles of War stand as an effective means to provide a level of clarity and insight into the operational capabilities of cyber. Cyber allows joint commanders to focus on an *objective* using more tools, to maintain an *offensive* spirit that further disrupts the enemy's decision cycle, to *mass* effects in conjunction with traditional methods, to *economize the use of force* while saving lives, to *surprise* the enemy with an instant first strike capacity, to leverage a less physically demanding form of *perseverance*, and to *maneuver* into areas without occupation. Additionally, the Principles of War highlight the fact that joint commands must still retain *unity of command* in the cyber domain, take adequate *security* measures to protect the force, and maximize the coordination of cyber operations through *simple* and logical courses of action.

Finally, just as in the years past, the Principles of War remind joint force commanders that they must use *restraint* to take advantage of opportunities presented by the enemy and to avoid the degradation of friendly capacity and always ensure cyber operations are conducted with the same *legitimacy* expected of all operations conducted on behalf of the United States. These principles do in fact apply to cyber operations and can increase our understanding of cyber war.

APPENDIX A: GLOSSARY

BOTNET: A collection of software agents, or robots that run autonomously and automatically.

Computer Intrusion: An incident of unauthorized access to data or an automated information system. (Joint Publication 3-13 Information Operations 13 February 2006)

Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Joint Publication 3-13 Information Operations 13 February 2006)

Computer Network Defense (CND): Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (Joint Publication 3-13 Information Operations 13 February 2006)

Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (Joint Publication 3-13 Information Operations 13 February 2006)

Computer Network Operations: Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. (Joint Publication 3-13 Information Operations 13 February 2006)

Economy of Force: The purpose of the economy of force is to allocate minimum essential combat power to secondary efforts. (Joint Publication 3-0 Joint Operations 17 September 2006, Incorporating Change 1, 13 Feb 2008)

Electronic Attack: The subdivision of electronic warfare where actions are taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception. EA uses electromagnetic energy, directed energy, and anti-radiation weapons to attack personnel, facilities or equipment with the intent of degrading, neutralizing, or destroying the enemy's combat capability. (Air Force Doctrine Document 2-X: Cyberspace Operations (Draft) 2009)

Hacktivism: Computer activism and operates in the tradition of non-violent direct action and civil disobedience. (Adkins April 2001)

Information Operations: The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (AFDD 2-5)

Intrusion Detection: The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practice.

Intrusion Detection System: A device (or application) that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

Intrusion Prevention: The process of performing intrusion detection and attempting to stop detected possible incidents.

Malicious Code: Software designed to infiltrate a computer system without the owner's informed consent.

Military Revolution: A radical military innovation that fundamentally changes the framework of war that renders former systems and methods obsolete or irreverent. These changes are cataclysmic events that occur infrequently that affect the social, political and military cultures and organizations. (Knox 2001)

Network Attack: The employment of network-based capabilities to destroy, disrupt, or corrupt information resident in or transiting through networks. (Air Force Doctrine Document 2-X: Cyberspace Operations (Draft) 2009)

Physical Attack: Uses kinetic means to physically destroy or otherwise adversely affect a target. (Air Force Doctrine Document 2-X: Cyberspace Operations (Draft) 2009)

Revolution in Military Affairs: RMAs can occur either separately or within the context of a larger military revolution. These "lesser transformations . . . appear susceptible to human direction, and in fostering them, military institutions that are intellectually alert can gain significant advantage". These changes typically affect only the military aspect of war. (Knox 2001)

Virus: A fragment of code that attaches itself to other computer instructions including software application code, the code used to boot a computer or macro instructions place in documents. When activated a virus may then execute a —payload" which can do anything from displaying an amusing message to wiping out files on the hard drive. (Adkins April 2001)

APPENDIX B: U.S. PRINCIPLES OF WAR DEFINED

Joint Publication 3-0, Joint Operations

Objective: The purpose of objective is to direct every military operation toward a clearly defined, decisive, and achievable goal. Changes to military objectives may occur because political and military leaders gain a better understanding of the situation, or they may occur because the situation itself changes.

Offensive: The purpose of offensive action is to seize, retain, and exploit the initiative. Offensive action is the most effective and decisive way to achieve a clearly defined objective. Offensive operations are the means by which a military force seizes and holds the initiative while maintaining freedom of action and achieving decisive results. The importance of offensive action is fundamentally true across all levels of war: tactical, operational, and strategic.

Mass: The purpose of mass is to concentrate the effects of combat power at the most advantageous place and time to produce decisive results. Mass often needs to be sustained to have the desired effect. Massing effects, rather than concentrating forces, can enable even numerically inferior forces to produce decisive results, minimizing human losses and waste of resources.

Economy of force: The purpose of economy of force is to allocate minimum essential combat power to secondary efforts. Economy of force is the judicious employment and distribution of forces. It is the measured allocation of available combat power to such tasks as limited attacks, defense, delays, deception, or even retrograde operations to achieve mass elsewhere at the decisive point and time.

Maneuver: The purpose of maneuver is to place the enemy in a position of disadvantage through the flexible application of combat power. Maneuver is the movement of forces in relation to the enemy to secure or retain positional advantage, usually in order to deliver — or threaten delivery of — the direct and indirect fires of the maneuvering force. Effective maneuver keeps the enemy off balance and thus protects the friendly force. It contributes materially to exploiting successes, preserving freedom of action, and reducing vulnerability by continually posing new problems for the enemy.

Unity of command: The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective. Unity of command means that all forces operate under a single commander with the requisite authority to direct employed combat power in pursuit of a common purpose.

Security: The purpose of security is to never permit the enemy to acquire unexpected advantage. Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise. Security results from the measures taken by commanders to protect their forces. Risk is inherent in military operations. Protecting the force increases friendly combat power and preserves freedom of action.

Surprise: The purpose of surprise is to strike at a time or place or in a manner for which the enemy is unprepared. Surprise can help the commander shift the balance of combat power and thus achieve success well out of proportion to the effort expended. Factors contributing to surprise include speed in decision-making, information sharing, and force movement; effective

intelligence; deception; application of unexpected combat power; operational security; and variations in tactics and methods of operation.

Simplicity: The purpose of simplicity is to prepare clear, uncomplicated plans and concise orders to ensure thorough understanding. Simple plans and clear, concise orders minimize misunderstanding and confusion. Simplicity and clarity of expression greatly facilitate mission execution in the stress, fatigue, and other complexities of modern combat and are especially critical to success in multinational operations, thus reduce the fog of war.

Restraint: The purpose of restraint is to limit collateral damage and prevent the unnecessary use of force. A single act could cause significant military and political consequences; therefore, judicious use of force is necessary. Restraint requires the careful and disciplined balancing of the need for security, the conduct of military operations, and the national strategic end state. Excessive force antagonizes those parties involved, thereby damaging the legitimacy of the organization that uses it while potentially enhancing the legitimacy of the opposing party.

Perseverance: The purpose of perseverance is to ensure the commitment necessary to attain the national strategic end state. Prepare for measured, protracted military operations in pursuit of the national strategic end state. Some joint operations may require years to reach the termination criteria. The underlying causes of the crisis may be elusive, making it difficult to achieve decisive resolution. The patient, resolute, and persistent pursuit of national goals and objectives often is a requirement for success. This will frequently involve diplomatic, economic, and informational measures to supplement military efforts.

Legitimacy: The purpose of legitimacy is to develop and maintain the will necessary to attain the national strategic end state. Legitimacy is based on the legality, morality, and rightness of the actions undertaken. Legitimacy is frequently a decisive element. Interested audiences may include the foreign nations, civil populations in the operational area, and the participating forces. Legitimacy may depend on adherence to objectives agreed to by the international community, ensuring the action is appropriate to the situation, and fairness in dealing with various factions. Restricting the use of force, restructuring the type of forces employed, and ensuring the disciplined conduct of the forces involved may reinforce legitimacy.

BIBLIOGRAPHY

Adkins, Maj Bonnie. “The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcements Role?” Master's thesis, Air Command and Staff College, Air University, April 2001.

Air Force Doctrine Document 1: Air Force Basic Doctrine. Washington D.C.: Department of The Air Force, 2003.

Air Force Doctrine Document 2-X: Cyberspace Operations (Draft). Washington D.C.: Department of the Air Force, 2009.

Alford, Lionel. “Cyber Warfare: Protecting Military Systems.” *The Journal of Defense Acquisition University Review* (Spring 2000).

Alger, Maj John. “The Origins and Adaptation of the Principles of War.” Master's thesis, Command General Staff College, 1995.

Ashmore, Maj William. “Impact of Alleged Russian Cyber Attacks.” Master's thesis, School of Advanced Military Studies, 2009.

Bosker, TSgt A.J. "SECAF: Dominance in cyberspace is not optional." *Air Force Print News Today* (55th WG Public Affairs), May 2007.

Burwell, Maj David. “Morale As A Principle of War.” Master's thesis, School of Advanced Military Science, 2000.

Capstone Concept for Joint Operations. Washington D.C.: Chairman of the Joint Chiefs of Staff, August 2005.

Capstone Concept of Joint Operations v 3.0. Washington D.C.: Chairman of Joint Chiefs of Staff, 15 Jan 2009.

Clausewitz, Carl Von. *The Principles of War*. Translated by Hans W. Gatzke. New York: The Military Service Publishing Company, 1942.

Clausewitz, Carl von. *On War*. Translated and Edited by Michael Howard and Peter Paret. West Sussex: Princeton University Press, 1976.

Cyber Effects: Analysis using VCSE. Sandia National Laboratories, September 2008.

Courville, Lt Col Shane. *Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future*. Occasional Paper No. 63. Maxwell AFB, AL: Center for Strategy and Technology, December 2007.

Davies, Owen, Stephen Steele, Cynthia Ayers, and Marvin Cetron. “World War 3.0: Ten Critical Trends for Cybersecurity.” *The Futurist* (September 2009).

“DoD Dictionary of Military Terms.” DoD Dictionary of Military Terms. http://www.dtic.mil/doctrine/dod_dictionary/index.html (accessed November 18, 2009).

Douhet, Giulio. *Command in the Air*. Translated by Dino Fer-ari. New York: Coward-McCann, 1942.

Eilperin, Juliet. "Hackers steal electronic data from top climate research center." *Washington Post*, 21 Nov 2009.

England, Gordon. The Definition of Cyberspace: Deputy SECDEF Memorandum to Secretaries of Military Departments. N.p.: May 12, 2008.

Espiner, Tom. “Georgia accuses Russia of coordinated cyberattack.” *CNET*, 11 August 2008.

Field Manual 3-0: Operations. Washington D.C.: Department of the Army, 2008.

Foch, Marshall Ferdinand. *The Principles of War*. Translated by Hillaire Belloc. New York: Henry Holt and Company, 1903.

Gates: Cyber Attacks a Constant Threat. April 21, 2009. http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml.

Grant, Rebecca. *Victory in Cyberspace*. Air Force Association Special Report. Arlington, VA: Air Force Association, October 2007.

Gray, Colin S. *The American Way of War*. Reading: University of Reading, 2005.

Hall, Camilla. "Mediterranean Cables Cut, Disrupting Communications." *Bloomberg.com*, 2008.

Holloway, Admiral James. *Special Operations Review Group: Iran Hostage Rescue*. Washington D.C.: Joint Chiefs of Staff, August 23, 1980.

Howard, Michael. *Clausewitz: A Very Short Introduction.* New York: Oxford University Press, 2002.

Huntington, Samuel P. The Clash of Civilizations and the Remaking of World Order. New York: Simon & Schuster, 1996.

“Internet Usage Statistics.” Internet Usage Statistics. http://www.internetworldstats.com/stats.htm (accessed March 15, 2010).

Joint Operating Environment 2008. Norfolk: United States Joint Forces Command, November 25, 2008.

Joint Operating Environment 2010. Norfolk: United States Joint Forces Command, February 18, 2010.

Joint Operations Insights and Best Practices. Norfolk: Joint Warfighting Center, July 2008.

Joint Publication 3-0 Joint Operations: 17 September 2006, Incorporating Change 1. Washington D.C.: Joint Chiefs of Staff, February 13, 2008.

Joint Publication 3-13 Information Operations. Washington D.C.: Joint Chiefs of Staff, February 13, 2006.

Joint Publication 3-30 Command and Control for Joint Air Operations. Washington D.C.: Joint Chiefs of Staff, January 12, 2010.

Joint Publication 3-31 Command and Control for Joint Land Operations. Washington D.C.: Joint Chiefs of Staff, March 23, 2004.

Joint Publication 3-32 Command and Control for Joint Maritime Operations: Incorporating Change 1 27 May 2008. Washington D.C.: Joint Chiefs of Staff, August 8, 2006.

Joint Publication 5-0 Joint Operating Planning. Washington D.C.: Joint Chiefs of Staff, December 26, 2006.

Joint Publication 6-0 Joint Communications System. Washington D.C.: Joint Chiefs of Staff, March 20, 2006.

Jomini, Baron de. *The Art of War*. Translated by Capt G.H. Mendall and Lt W.P. Craighill. West Point: US Military Academy, 1862.

Knox, MacGregor, and Williamson Murray. *The Dynamics of Military Revolution 1300-2050*. Cambridge: Cambridge University Press, 2001.

Leonhard, Robert. *The Principles of War for the Information Age*. Novato, CA: Presidio Press, 2000.

Lyle, Tech. Sgt. Amaani. *SecAF Delivers 'State of the Air Force' speech at AFA.* Secretary of the Air Force Public Affairs, September 14 2009.

Merriam-Webster Online. http://www.merriam-webster.com/ (accessed March 22, 2010).

Miles, Donna. "Gates Establishes New Cyber Subcommand." *American Forces Press Service* (June 24 2009).

National Military Strategy for Cyberspace Operations. Washington D.C.: Joint Chiefs of Staff, December 2006.

National Strategy to Secure Cyberspace. Washington D.C.: White House, February 2003.

Nye, Jr., Joseph. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs, 2004.

Osterholz, John. "Data Bombs Away." *Armed Forces Journal* (September 2009).

Paret, Peter. Makers of Modern Strategy from Machievelli to the Nuclear Age. Princeton: Princeton University Press, 1986.

Piatt, Maj Walter. "Do the Principles of War Still Apply?" Master's thesis, School of Advanced Military Studies, 1999.

Quadrennial Defense Review 2010. Washington D.C.: Secretary of Defense, February 2010.

Quadrennial Defense Review 2006. Washington D.C.: Secretary of Defense, 2006.

Scherrer, Lt Col Joseph, and Lt Col William Grund. *A Cyberspace Command and Control Model*. Montgomery, AL: Air University Press, 2009.

Spies Penetrate U.S. Electrical Grid. April 8, 2009. http://www.cbsnews.com/stories/2009/04/08/national/main4928223.shtml?source=related_story.

The National Security Strategy of the United States of America. Washington D.C.: The White House, 2006.

"Twitter Links Iran Protesters to Outside World." *foxnews.com*, 16 June 2009.

Tzu, Sun. *On the Art of War*. Translated by Lionel Giles. N.p.: 1910.

Unified Command Plan 2008. Washington D.C.: Secretary of Defense, 2008.

West, Robert C. "The Cyber-defence Force's Virtual Shield." *Janes Intelligence Review* (December 2000).

Westenhoff, Lt Col Charles. *The CADRE Digest of Air Power Opinions and Policy Issues*. Maxwell AFB, AL: Air University, October 1990.

Wilson, Clay. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Washington D.C.: Congressional Research Service, January 29 2009.