Wired Fast and Thinking Slow:
Cyber Technology and the US Army

A Monograph

by

Major Johanna Thompson Wynne
US Army

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

2016

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-05-2016	Monograph	JUN 2015 - MAY 2016

4. TITLE AND SUBTITLE
Wired Fast and Thinking Slow : Cyber Technology and the US Army

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Johanna Thompson Wynne

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies, Advanced Military Studies Program

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Understanding the impacts of cyber technologies on war and warfare is increasingly critical for a planner's ability to design and execute operational art. The purpose of this monograph is to examine how the US Army describes cyberspace and the effects that cyber technologies have on military strategy and operational planning writ large. The work specifically examines how cyberspace increases the speed and quantity of social transactions over space with effects on military and social forces. Secondly it addresses how the Army recognizes the impact of cyber technology on identity formation and virtual identity of both friendly and enemy actors. The author concludes that society's and the Army's increasing dependence and activity in cyberspace marks a change in warfare that the Army has been slow to accept. Inadequate coverage of the implications of cyberspace throughout doctrine combined with insufficient emphasis in professional military education and training may limit the Army's potential in all levels of war.

15. SUBJECT TERMS
Cyber, Cyberspace, Technology, Operational Art, Cyber Planning, Domain, Virtual Identity, Space, Time, Strategy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			MAJ Johanna Thompson Wynne
(U)	(U)	(U)	(U)	56	19b. TELEPHONE NUMBER *(Include area code)*

Reset

Monograph Approval Page

Name of Candidate:	Major Johanna Thompson Wynne
Monograph Title:	Wired Fast and Thinking Slow: Cyber Technology and the US Army

Approved by:

_____, Monograph Director
Alice Butler-Smith, PhD

_____, Seminar Leader
Christopher M. McGowan, COL

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

Accepted this 10th day of May 2016 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

Abstract

Wired Fast and Thinking Slow: Cyber Technology and the US Army, by MAJ Johanna Wynne, 56 pages.

Understanding the impacts of cyber technologies on war and warfare is increasingly critical for a planner's ability to design and execute operational art. The purpose of this monograph is to examine how the US Army describes cyberspace and the effects that cyber technologies have on military strategy and operational planning writ large. The work specifically examines how cyberspace increases the speed and quantity of social transactions over space with effects on military and social forces. Secondly it addresses how the Army recognizes the impact of cyber technology on identity formation and virtual identity of both friendly and enemy actors. The author concludes that society's and the Army's increasing dependence and activity in cyberspace marks a change in warfare that the Army has been slow to accept. Inadequate coverage of the implications of cyberspace throughout doctrine combined with insufficient emphasis in professional military education and training may limit the Army's potential in all levels of war.

Contents

Acknowledgments…….....v

Acronyms……vi

Figures…….....vii

Introduction……...……1

Method……...…….....……3

Review of Terms and Literature…….....……4

The Importance of the Outcome ……..…….…..….....11

A Critical Illustration…….……...…….....16

Cyberspace and the Operational Artist……...19

The First Condition of Adequacy: Accounting for Time and Space in the Contemporary Operating Environment…….....…..20

The Fixing of Space in War.……...……...……26

Time and Decision Time…….…...……...…….28

Virtual Space and the Future of War……..……...……29

Broadening the Army's Conception of Cyberspace…….....……...…….35

The Second Condition of Adequacy: Emphasis on Techno-Social Relations…….....…...38

Army Understanding of Real and Virtual Identity: What's in a Name? ……..…….……40

The Digital Immigrant and Digital Native Divide……44

Artificial Intelligence and the Army…….....45

Conclusion……...……...46

Bibliography……...50

Acknowledgments

This monograph is largely inspired by my fourteen year old protégé Jasmine Del Cid Reyes. I am indebted to Dr. Gene Rochlin for our correspondence throughout this journey and the Combined Arms Resource Library for carrying his and many other valuable works. A special thanks to Dr. Alice Butler-Smith for her initial and lasting belief in me and for her impact on the School of Advanced Military Studies. I am grateful for my seminar leader, Colonel McGowan for his thoughtful guidance and patience throughout the course of the year. To Drew and Laura Brooks, thank you for being the best neighbors. The greatest recognition goes to my husband Brian, son John, my parents Linda and John, and my sister Heather – you make all things possible and worthwhile. I love you.

Acronyms

ADRP	Army Defense Reference Publication
CJTF	Combined Joint Task Force
CO	Cyber Operations
DARPA	Defense Advanced Research Project Agency
DOD	Department of Defense
GPS	Global Positioning System
IS	Islamic State
MRI	Magnetic Response Imaging
NSDD	National Security Decision Directive
OCO	Offensive Cyber Operations
OIR	Operation Inherent Resolve
PTSD	Post Traumatic Stress Disorder
VR	Virtual Reality

Figures

1 If the Titanic Sank In 2015 24

Introduction

I AM a copper wire slung in the air,
Slim against the sun I make not even a clear line of
shadow.
Night and day I keep singing--humming and thrumming:
It is love and war and money; it is the fighting
and the tears, the work and want,
Death and laughter of men and women passing through
me, carrier of your speech,
In the rain and the wet dripping, in the dawn and the
shine drying,
A copper wire.

— Carl Sandberg, *Under A Telephone Pole*

Throughout recorded history, individuals and societies have had a fascination and a complex relationship with technology. Carl Sandberg's poem, "Under a Telephone Pole," is one such example from the twentieth century. The work personifies a telephone wire as being aware of its disparate uses—coursing with conversations that vary in substance[1]— a tangible wire, essential for modern communication, considered ubiquitous, and taken for granted. Sandberg's poem illustrates the paradoxical nature of technology.

Prior to the electric telegraph, the speed of almost all information flow was limited to the speed at which a human or animal could travel.[2] In 1858, the first transatlantic messages traveled between Europe and North America via underwater telegraph cables. This cable signaled the reduction of information transmission time from days to hours in the transatlantic space.[3] Along with other technological advances in power and transportation, the transatlantic telegraph freed communication from the constraints of space

[1] Carl Sandburg, *Chicago Poems* (New York: Henry Holt and Company, 1916), 171.

[2] "1830s-1860s: The Telegraph," Imagining the Internet, A History and a Forecast, Elon University, accessed 30 March 2016, http://www.elon.edu/e-web/predictions/150/1830.xhtml.

[3] Barney Warf, *Time- Space Compression* (New York: Routledge, 2008), 168

and time and occasioned a revolution in the global economy and social order. For many, the increased scale of economic, diplomatic, and social interdependencies seemed to presage the inevitability of world peace.[4] Instead, two world wars, a cold war, and scores of regional and local wars marked this unrealized vision.

Though underwater cables similar to those used by the first transatlantic telegraph endure as a critical element in the twenty-first century global communications infrastructure, wireless cyber technology now connects people, things, and systems virtually and instantaneously from and to locations across the globe. The pace of life continues to increase as perceptions of physical distances and time contract in a world simultaneously enlarged and shrunk by technology. Exponentially rapid technological progress now inspires utopian hopes similar to those generated by the telegraph, yet war perseveres as part of human experience. [5]

The role of cyber technology in society has changed profoundly over the last decades. Not only is it being used for a wide array of applications, it is also at the same time embedded in our environment, often present largely without user awareness. With a rapidity unprecedented in previous revolutions in technology, cyber technology has become increasingly involved in decisions that have moral impact, such as war. The push for faster and enhanced methods of communication, information processing, and simulated activity continues to define and shape global action and conflict. Despite the worldwide use and pervasiveness of cyber technology, there is little consensus—within the US Army or broader society—on how cyber technology should be understood and conceptualized. Is it a means to democratize or way to

[4] Paul Reynolds, "The Man Who Predicted the Great War," *History Today* 20, no. 2 (2013), accessed 24 March 2016, http://www.historytoday.com/paul-reynolds/man-who-predicted-great-war. Financier Jan Bloch outlined his vision to Britain's military establishment in 1901. Earlier in 1899 at the Hague, he called for arbitration to replace warfare as a way to settle disputes.

[5] Dex Torrike-Barton, "How the internet is uniting the world," A Medium Corporation, October 14, 2015, accessed, October 14, 2015, https://medium.com/@dextbarton/how-the-internet-is-uniting-the-world-36408b457692#.7uzz7i54n.

control? Does it diffuse or consolidate power? Do people define the technology or does the technology define people? To each of these questions, the answer is yes.

The Army's initial attempts to create and clarify doctrine related to cyberspace operations, to establish a cyber branch, and to develop elite cyber warriors are positive steps, but may effectively limit the organization's ability to address the broader significance and strategic potential of cyberspace.[6] Military discourse reveals little examination of political theory, social theory, and other foundational frameworks of relevance for exploring this most transformative time in human history, even though. the nature of cyberspace, the full potential of cyber operations, and the long-term societal effects are self-evidently of military concern.

The Method for Demonstrating the Need

A proof of inadequacy must always start with certain assumptions about what is adequate in the first place. This work proposes that notions of cyberspace as related to the development of military strategy are observationally and descriptively adequate when they include, at a minimum, the following two assertions: [7]

Condition of Adequacy #1: This requires in-depth treatment of the variables of time and space as related to the contemporary operating environment. Conceptualizations of cyberspace must meet this condition because cyber technology facilitates the increased speed and quantity of social transactions over space, thus compressing cognitive understandings of time and space with effects on military, political, cultural, economic, and ideological forces.[8]

---

[6] Victor Delacruz, "Enabling Army Commanders to More Effectively Integrate Cyberspace Operations," *Cyber Compendium: Cyberspace Professional Continuing Education Course Papers* (Wright-Patterson Air Force Base, OH, 2015): 110-118.

[7] For further discussion of the concepts of observational, descriptive, and explanatory adequacy in scientific theory, see Noam Chomsky, *Syntactic Structures* (The Hague: Mouton, 1957).

[8] Barney Warf, *Time- Space Compression* (New York: Routledge, 2008), 168.

Condition of Adequacy #2: This requires proper weighting of the relationship between cyber technology and human behavior from both friendly and adversarial perspectives. It must meet this condition because cyber technology continues to alter how individuals and societies construct reality and expressions of life today and in the future.

The purpose of this monograph is to determine whether the US Army's current construction of cyberspace in informing military strategy meets these conditions of adequacy. The paper uses two research questions to demonstrate its intent:

The first question considers how the Army accounts for the fundamental concepts of time and space, especially as related to cyberspace and the execution of operational art. The second question asks how the Army recognizes the role that cyberspace plays in identity formation and the social constructions of reality of both friendly and enemy actors.

The work has four sections. The first section begins with the introduction and method and concludes with key terms in the research and a review of definitive literature. Section two illustrates the complexity of cyberspace for the military practitioner and provides analysis of how cyber technology compresses cognitive understandings of time and space with effects on the contemporary operating environment and operational art. The third section examines the significance for both friendly and enemy actors of cyber technology's effects on the construction of identity and virtual identities. The fourth and final section concludes the work by highlighting the implications of conceptualizing cyberspace according to these conditions of adequacy and makes explicit recommendations to broaden strategic thinking into existing core Army doctrine and force structures. Potential lines of further inquiry of these and related topics are included throughout the work.

Review of Terms and Literature

Given the enormity of the literature dealing with cyber technology, sufficiency rather than relevance guides this section of the monograph.[9] The research draws on literature from several disciplines in its exploration of the concepts related to time, space and identity. The review reaches sufficiency when it finds descriptive evidence or analysis that persuasively addresses how the Army conceptualizes cyberspace in time and space and how cyber technologies affect individuals and society. Four prominent themes from military, historical, social science, and technology perspectives emerge to help answer the research questions posed.

Key Terms

Numerous definitions have emerged to describe computer networking and related phenomena over the past few decades. For example, in the years since the development of the first cyber networks in the late nineteen sixties, the US Department of Defense has issued at least twelve different definitions of what it thinks of as cyberspace.[10] Furthermore, terms used to describe cyberspace are understood to mean different things by different nations and organizations, despite their commonness in media, national and international organizational policies and programs, and in everyday speech.[11]

A generation ago, writer William Gibson first coined the term cyberspace in his science fiction novel, *Neuromancer*. He combined the word cybernetics and space to describe his concept of cyberspace as "a graphic representation of data abstracted from the banks of every computer in the human system.

[9] In other words, *sufficient* to prove the point, not *all* that may be *relevant.*

[10] P.W. Singer and Allan Friedman, *Cybersecurity and CyberWar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 16.

[11] "Cyber Definitions," NATO Cooperative Defence Center of Excellence: Tallin, Estonia, accessed March 10, 2016, https://ccdcoe.org/cyber-definitions.html.

Lines of light ranged in the nonspace of the mind, clusters and constellations of data."[12] Joint and Army doctrine currently hold that cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[13] US National Security experts have referred to cyberspace as "like a game of global chess, wherein the players are unsure who else is playing, uncertain of friend or foe, unclear about the terrain and unconvinced the players will act according to established rules and norms."[14] These multiple definitions of cyberspace and the elements that comprise them have done much to challenge the Army's current comprehension and operationalization of cyberspace.

It is useful then to address here how *this* monograph defines cyber and related key terms. The word *cyber* is generally believed to originate from the Ancient Greek verb κυβερεω (kybereo), "to steer, to guide, to control."[15] Today, it is often the prefix for a term or the modifier of a compound word. Its inference usually relates to electronic information (data) processing, information technology, data transfer, or information and computer systems. An example of its misapplication is in such guidance to offensive cyber operations (OCO) planners within the conventional operations community as "I want to

[12] Peter Singer, introduction to "Gen. Dempsey's Remarks and Q&A on Cyber Security at the Brookins Institute," Joint Chiefs of Staff Speech Archive, July 27, 2013, accessed September 28, 2015, http://www.jcs.mil/Media/Speeches/tabid/3890/Article/571864/gen-dempseys-remarks-and-qa-on-cyber-security-at-the-brookings-institute.aspx and William Gibson, *Neuromancer* (New York: Berkley Publishing Group, 1989), 128.

[13] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, 2011; Field Manual (FM) 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Government Printing Office, 2014), 3-3.

[14] Frank L.Turner, "The Army in Cyberspace," National Security Watch 14-1, Institute of Land Warfare, May 5, 2014, accessed March 16, 2016, http://www.ausa.org/publications/ilw/Digital Publications/Documents/nsw14-1/files/1.html. The analogy was collectively developed at the Information Environment Advanced Analysis Course (IEAA) in October 2012.

[15] "Cyber Definitions," NATO Cooperative Defence Center of Excellence: Tallin, Estonia, accessed March 10, 2016, https://ccdcoe.org/cyber-definitions.html.

do some cyber here."[16] Only a complete term that includes *cyber* as a prefix or compound element can be considered to possess operational meaning.

Cyberspace is composed of the information and connections in a virtual space that is in fact grounded in the physical world of hardware and software and dependent on human design and maintenance. Despite their common conflation, the *Internet* is a distinct, smaller subset of the larger cyberspace. Although everything connected to the Internet connects to cyberspace, the converse is not true. This is an important distinction as there are many interdependent networks of infrastructures that are not part of the Internet that include air gapped systems and embedded processors and controllers in a range of platforms from cars to satellites.[17] *Cyber technology* is defined as the physical computer hardware and software systems that contribute to the creation of cyberspace. A *cyber capability* is a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.[18] It is possible, that over time, these varied terms may become more universally defined and understood. Until then, or in the case that does not occur, the US Army must ensure its leaders across *every* branch work to understand the basic nuances of language used to describe cyber technology and cyberspace.

Literature

The study of cyberspace as related to military doctrine and strategy is a developing field of inquiry and, thus, requires research from multiple disciplines. The first theme of this monograph includes

[16] Jason Bender, "The Cyberspace Operations Planner," *Small Wars Journal* November 5, 2013. Bender explains, "As funny as it might sound, this is not different than providing guidance "to do some logistics during Phase 2," or my intent is to reinforce the airborne insertion by doing some Air Force."

[17] The employment of the Stuxnet virus may be the most well-known state sponsored example of an air gapped virus.

[18] Field Manual (FM) 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Government Printing Office, 2014), 3-3.

the work of national security experts and military practitioners. Articles from the Center for Strategic & International Studies, Joint Force Quarterly, the US Army War College Strategic Studies Institute, Military Review, the Small Wars Journal and the Cyber Defense Review demonstrate that military practitioners largely view cyber technology as a capability that is to be integrated into hierarchical, industrial age paradigms of understanding. Many works address adversarial threats to physical networks and critical infrastructure. The foci in over ten articles associated with the above publications were related to frustrations in operationalizing cyberspace, and/or incorporating cyber operations more fluidly at the operational and tactical level. A majority of the handful that did address limitations associated with the lack of a comprehensive cyber strategy attributed this largely to the complex nature of the domain.

In his work *Team of Teams,* General Stanley McCrystal offers another perspective as he argues that the military must break away from a tradition of "predictive hubris, perhaps bred by centuries of success at applying Newtonian models to complicated problems," which has led the organization to have a false sense of control.[19] Dr. Timothy Thomas's work, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic," provides a strong case that cyber technologies are creating a new strategic paradigm that the DOD needs to understand and adapt to. In pointed consideration of the unprecedented operational challenges and opportunities that cyberspace presents he concludes that a cyber task force of many experts is required to implications of the military and society's increasing dependence on cyber technologies.[20]

The research within the military category also consults cyber specific US Joint and Army doctrinal publications. The study of these point to the indication that the Army primarily thinks about cyberspace in tactical terms, as a capability. The final military themed works include TRADOC Pamphlet 525-3-1, *The Army Operating Concept* (AOC), Army Defense Reference Publication (ADRP) 3-0,

---

[19] Stanley McCrystal, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin, 2015), 74.

[20] Tim Thomas, "Creating Cyber Strategists: Escaping the 'DIME,'" *Mnemonic, Defence Studies* 14, no. 4 (2014): 370, accessed January 5, 2016, http://dx.doi.org/10.1080 /14702436.2014.952522.

Unified Land Operations; ADRP 3-90, *Offense and Defense*, ADRP 5-0, *The Operations Process*, and ADRP 6-0, *Mission Command*. Overall, this collection suggests that significant gaps exist in the Army's ability to appreciate and pursue the full scope of the cyber domain.

The next source of research considers the work of historians interested in using past experience to search for reflections of things to come. Johnny Ryan's *A History of the Internet and the Digital Future* tells the story of the development of the internet from the 1950s to the present and informs this author's insight into technology's conceptual compression of time and space. This work also provides examples of how cyber technology affects the balances of power between the individual and the state. Martin van Creveld's *Technology and War* and Annie Jacobsen's *The Pentagon's Brain: An Uncensored History of DARPA, America's Top Secret Military Research Agency* provided additional historical windows on the influence of previous technical innovations on society and war. Numerous historical references within these and other historical works offered examples of how social effects of previous technologies are often misestimated or underexplored.

The third category of research is comprised of technological futurists who attempt to project future trends given their subject matter expertise and, in some cases, their personal desire to influence world outcomes.[21] Prominent in this category is *The New Digital Age* by Google founders and executives Eric Schmidt and Jared Cohen, who offer a prescriptive glimpse into how cyber technology is reshaping warfare, the world, and the lives of people within it. Their work addresses their understanding of virtual and physical identity today and in the future. They also provide specific examples of how virtual space fails to parallel physical space perfectly, causing significant geopolitical confusion as related to the defining of norms and in the attribution of hostile activities in cyberspace to state or nonstate actors. Futurist P.W. Singer's book *Wired for War*, his recent testimony to Congress, and several of his articles

[21] Mark Zuckerberg of Facebook, Steve Jobs of Apple, Jeff Bezos of Amazon, and Elon Musk of Tesla are a few such examples.

dealing with the unique relationship between current technological advances and the future of war are also key references.

This collection of works indicates that the pace of technological change is likely to remain a challenge for military planners in the years to come. They also demonstrate there are individuals with command of and investment in powerful cyber technologies with which they will actively work to shape the conditions of the future. Given that the future outcomes are in the long term unknowable and that the effects of their activities are largely unpredictable, this paradox further demonstrates that a most broadly grounded understanding of the potentials associated with cyber technology will provide the Army the best chance of coping with uncertainties as they emerge.

Finally, the fourth group of research includes academic and think-tank works of social scientists dealing with philosophy, anthropology, geography, international relations, and postmodern theory. These works examine how previous technologies and cyber technologies transform human experience across dimensions of temporality, spatiality, embodiment, and sociality. Prominent in this grouping is *Trapped in the Net: The Unanticipated Consequences of Computerization* by Gene I. Rochlin, who examines how the pervasive effects of cyber technology have become embedded in society creating many unforeseen and increasingly unmanageable outcomes. Barney Warf's work *Time-Space Compression: Historical Geographies* provides a deep analysis of geography, time, and space and an understanding of pre-modern, modern, and postmodern thought. Also within this fourth group of social scientists are works by Clay Shirky and Sheryl Turkle, both of whom attempt to examine the social effects in societies that increase their cyber technological dependencies.

International relations expert James Der Derian's work *Virtuous War: Mapping the military–industrial-media entertainment network*, Adam Segal's, *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age* and Henry Kissinger's *World Order* are the political science works prominent in this category. Segal argues that cyber conflict demands that rules of engagement be completely reworked and all the "old niceties of diplomacy be recast." He also addresses the fact that many of the critical resources of statecraft are now in the hands of giant technology

companies.[22] Kissinger argues: "Cyberspace challenges all historical experience."[23] In his view, the influence of cyber technology on strategy and decision making has eclipsed knowledge and wisdom.[24] These works demonstrate the unique and emergent role of cyberspace on and between actors and the discomfort of many in dealing with the challenges of the domain. In sum, the study of cyber technology through the lens of multi-disciplinary research is and will continue to be critical to understanding how and why the Army understands cyberspace and its role in war.

The most significant limitation of this monograph is its range. The investigative questions arguably constitute a mega-topic. Therefore, there is a vast amount of literature and research production that the manuscript necessarily ignores, leaving the danger—indeed the likelihood— that within the ignored material lies a critical nugget. The research scope itself is limiting because it is impossible to provide coverage for the myriad existing cyberspace related opportunities and challenges.

Most military practitioners assert that war is an inherently human experience—a contest of wills, one that technology alone will not change.[25] However, growing evidence provided by other disciplines demonstrates cyber technology's tremendous influence on social understanding and life meaning, which at a *minimum* constitutes the potential for significant changes in the execution of warfare. It falls to the Army to act deliberately and aggressively to understand the implications of these changes for every level of war. As of 2016, no prevailing US military cyber theory exists.[26] Through an examination of cyber

---

[22] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age* (New York: Public Affairs, 2016), 15.

[23] Henry Kissinger, *World Order* (New York: Penguin Books), *344.*

[24] Ibid.

[25] Army Doctrine Publication (ADP)1-01, *Doctrine Primer* (Washington, DC: Government Printing Office, 2014).

[26] Sean Charles and Gaines Kern, "Expanding Combat Power Through Military Cyber Power Theory," *Joint Force Quarterly* 79 (4th Quarter 2015), 88-94.

technology's impact on modern conceptions of space, time, identity, and what this means for the military, this work is meant to contribute to the construction of such a theory.

The Importance of the Outcome

The explosion in the use of cyberspace by individuals and communities across the globe both supports and challenges the military's comprehension of its operational environment in depth and scale. Part of the gap in current understanding of the operational environment relates to how cyber technologies were originally introduced to society. The Internet, for example, was designed to be open, transparent and interoperable with security and identity management as secondary objectives in system design.[27] The roots of cyber technical related opportunities and challenges were identified decades ago by prescient innovators, academics, members of the Department of Defense and even the White House. For example, as early as 1984, President Reagan, issued a confidential national security decision directive (NSDD), NSDD-145, titled "National Policy on Telecommunications and Automated Information Systems Security." In it, the government noted computers as "highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation" by hostile foreign intelligence agencies, terrorist groups, and criminal elements.[28]

Less than a decade later, in 1992, Department of Defense leaders issued DOD Directive TS3600.1, which stated that the central role of information in modern warfare (a) requires that US forces be prepared to operate in an information-hostile environment, (b) cautions not to plan to fight in ways that require more bandwidth than can be protected, (c) instructs commanders to understand the impact to

[27] Paul Rosenzweig, "Cyberwar is Here to Stay," George Washington University, February 24, 2016, accessed March 6, 2016, http://www.governing.com/templates/ gov_print_article?id=370008341.

[28] NSDD 145 National Policy on Telecommunications and Automated Information Systems Security, September 17, 1984, National Archives Catalog, accessed January 15, 2016, https://research.archives.gov/id/6879742.

forces under their command if they are denied the information they expect to have, and (d) to train in ways that gain an appreciation of their degree of information dependency.[29]

Despite identification of US vulnerabilities and adversarial opportunities associated with computing well prior to dependency at the institutional level, the government did not emphasize security in hardware, software, or network design; nor did it invest heavily in the study of the related social implications of the nation's increasing reliance on cyber technology.[30] In part, the explanation for this lack of investment by the government and the military lies with the already mentioned rate at which cyber technologies develop and deploy. Their extremely rapid pace routinely cuts short or prevents necessary conversation regarding its effects on people, organizations, and society.

In 1997, Rochlin wrote, with great foresight,

> The United States is now on the verge of being fully committed to a military that is fully interconnected horizontally and vertically, without any real sense of what the increased dependence on information management, data flows, real-time battle management, and other manifestations of the computer transition will do either to organizational structure and behavior or to performance in combat.[31]

Again, this prescient assessment was made well before the military's exponential increase in use and capability of mobile devices and nearly a decade before the launching of successful and now pervasive social media platforms.[32]

In his fiscal 2017 budget proposal, President Barack Obama asked for nineteen billion dollars in budgeting for cyber domain related activity across the US Government, a five billion dollar increase from

---

[29] Ronald J. Knect, "Thoughts About Information Warfare," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, eds. Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden (Fairfax, VA: Armed Forces Communications and Electronics Association), 162.

[30] Craig Timber, "Net of Insecurity: A Flaw in the Design," *The Washington Post*, May 30, 2015, accessed February 15, 2016, http://www.washingtonpost.com/sf/business/2015/05/30/ net-of-insecurity-part-1/.

[31] Gene I. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton, NJ: Princeton University Press, 1997), 191.

[32] Examples include Facebook, Twitter, Snapchat, Instagram, Kik, WhatsApp.

the previous year.[33] The Department of Defense fights for funding and resources to achieve the government's priorities and, therefore, military leaders are increasingly expected to incorporate cyberspace operations as part of planning at all levels of war.[34] It follows that Army leaders are obliged to study and help evaluate the effects of cyber technology on both the military and society to be able to provide informed assessments and options to senior Army leaders and political decision makers.

Futurists Alvin and Heidi Toffler have long argued that the way in which a society makes war reflects the way it makes wealth.[35] Historian Peter Paret has advised that war should be studied in the shifting reality in which it occurs.[36] Strategist and military practitioner Carl von Clausewitz declared,

> We can thus only say that the aims a belligerent adopts, and the resources he employs, must be governed by the particular characteristics of his own position; but they will also conform to the spirit of the age and to its general character. Finally, they must always be governed by the general conclusions to be drawn from the nature of war itself.[37]

However, many, if not most, uniformed Army service members lack a fundamental understanding of not just the technical aspects of cyberspace activity, but also the political, economic, and social implications. As military decision makers are unprepared to answer questions associated with *what* cyberspace is or *how* to conduct cyberspace operations, they are equally unable to assess the related

---

[33] White House Fact Sheet: Cybersecurity National Action Plan https :// www. whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, accessed March 11, 2016.

[34] Department of Defense 2017 Budget Fact Sheet http://www.defense.gov/Portals/1/features/2016/0216_budget/docs/2-4-16_Consolidated_ DoD_FY17_Budget_Fact_Sheet.pdf, accessed March 11, 2016.

[35] Alvin Toffler and Heidi Toffler, *War and Anti-War* (New York: Warner Books, 1995), 57-80.

[36] Peter Paret, *The Cognitive Challenge of War* (Princeton: Princeton University Press, 2009), 5.

[37] Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. (Princeton: Princeton University Press, 1984), 718.

questions of what *should* we do and perhaps, most important, *why*?[38] Increasingly prevalent conflict in cyberspace and US society's willful and perhaps unavoidable submission to surveillance by corporate-owned cyber technologies forms the background against which the positivist organizational culture of the Army continues to allow reductionist thinking and illusions of control, based on traditional models of planning and prediction.[39] Yet the intensifying global interdependence on cyberspace bears on more than the employment of Army's cyber capabilities.

Cyberspace is hypercomplex and arguably beyond individual comprehension; it is infinite, therefore, in the same practical sense as are the moves on a chessboard.[40] Priority efforts to improve understanding of this contemporary reality verses limiting the study of their significance is a first step in developing the real strategic potential of cyber technology in war. Broadening the conceptualization of cyberspace beyond specific cyber operational capabilities performed by unique military occupational specialties or branches within services will accelerate urgently needed understanding and emphasis across the force. In order for the United States to achieve and maintain positions of strategic, operational, and tactical advantage in warfighting and for it to exploit the shifting power dynamics writ large, there comes a growing, critical need for Army soldiers across all branches to acquire and participate in a mindset that apprehends the fullest reach and potentiality of cyberspace in affecting every military niche from the recruitment and training of the force to the successful execution of operational art.

---

[38] Martha S.H. VanDriel "Bridging the Planning Gap: Incorporating Cyberspace Into Operational Planning," *Strategic Studies Institute*, May 4, 2015, accessed December 10, 2015, http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Bridging-the-planning-gap/2015/05/04.

[39] McCrystal, 79; Rochlin, 191.

[40] For purposes of familiarity the chess example is provided but the game of "Go" is even more hypercomplex. In chess, the number of legal moves a player can make each turn is, on average, 35. In Go, that number is 250.Even the computer that mastered Go could not solve it; it only outmaneuvered the human champion it beat.

Living within such rapid change makes the mere recognition of the tremendous and unknown consequences very difficult, but very important to achieve at a practical level. [41] Throughout much of its history, US military strategy and doctrine has set a premium on trying to prepare for and anticipate the dimly perceived outlines of the "shape-of-things-to-come" future. [42] Because of the accelerated advancements in cyber technology, even what can dimly be perceived as an outline of an anticipated future quickly recedes into unrecognizable white noise.

A minimum requirement in designing successful operations is an appreciation of war's indistinct nature against an overwhelming tendency to try to control it. The effect of bureaucratizing the domain of strategic planning for using and protecting cyber technology – with self-perpetuation the primary goal of every bureaucracy –is "largely ignored until made glaring clear by the un-strategic, ambiguous and often non-substantive official documents laid out by and for them."[43] While the nature of war may be timeless, history demonstrates that its rules are not stagnant. Cyber technologies engender new questions, which require new rules and new approaches.[44] The Army must now indeed play "catch up."

A Critical Illustration

[41] "US Cybercom and the NSA: A Strategic Look with ADM Michael S. Rogers," Atlantic Council Commanders Series Event, January 21, 2016, accessed on January 25, 2016, http://www.atlanticcouncil.org/events/webcasts/us-cybercom-and-the-nsa-a-strategic-look-with-adm-michael-s-rogers.

[42] *The Shape of Things to Come* is a work of science fiction by H. G. Wells, published in 1933, which speculates on future events from 1933 until the year 2106. In the book, a world state is established as the solution to humanity's problems.

[43] Joan Johnson-Freese, "Domains, Budgets and Bureaucracies: Nukes, Space & Now — Cyber," *Breaking Defense*, October 24, 2014, accessed March 26, 2016, http://breakingdefense.com/2014/10/domains-budgets-and-bureaucracies-nukes-space-now-cyber/

[44] James Der Derian, "Virtuous War/Virtual Theory," International Affairs (Royal Institute of International Affairs 1944-), 76, No.4 (2000), 771-778, accessed February 29, 2016, http://www.jstor.org/stable/2626459.

In February 2016, Facebook inventor and Chief Executive Officer, Mark Zuckerberg encouraged the world to share on his social network "what they're thinking about, what they're experiencing on a day-to-day basis, and the idea is that everyone has the power to share those things, then that makes the world more understanding, it helps people stay closer to the people who they love, all these good things that we value."[45] Facebook is obviously not a physical country, but with 1.6 billion users, the service has a "population" larger than the world's most populous nations of China and India. While Facebook is unable to tax or jail its inhabitants, its executives, programmers, and engineers do exercise a form of governance over people's online activities and identities.[46] Notably, for purposes of this work, Mr. Zuckerberg's message has evidently been interpreted and taken to heart by the Islamic State of Iraq and the Levant (ISIL) or Daesh, despite recent efforts by the US and Coalition militaries and Silicon Valley to exclude the group from Facebook's family and from other popular social media platforms.[47]

Daesh's hacking unit, "Sons of the Caliphate Army," recently boasted to the leadership of Facebook, Twitter, and the US government of their more than 10,000 Facebook accounts, 150 Facebook groups, and 5,000 Twitter accounts.[48] Though the terrorist organization's numbers and capabilities are likely inflated, truth rests in eye of the beholder, and the group's enticing messages to the disenfranchised,

---

[45] Barbara Kollmeyer, "Want World Peace? Share much more on Facebook, Mark Zuckerberg says," *Marketwatch*, February 26, 2016, , accessed March 16, 2016, http://www .marketwatch.com/ story/facebooks-mark-zuckerberg-touts-more-sharing-as-a-route-to-world-peace-2016-02-26.

[46] Rebecca McKinnon, "Ruling Facebookistan: The world's largest social networking site has a population nearly as large as China or India's. And the natives are getting restless," *Foreign Policy Magazine*, June 14, 2012, accessed March 25, 2016, http://foreignpolicy.com/2012/06/14/ ruling-facebookistan/.

[47] Anthony Cuthbertson "US Military Launches Cyberattacks against ISIS," *Newsweek Magazine*, March 2, 2016, http://www.newsweek.com/us-military-launches-cyber-attacks-isis-432441accessed March 2, 2016. ISIL would prefer to be referred as "Islamic State." The term *Daesh* is considered uncomplimentary, but is used in addition to ISIL, however, by the US government.

[48] William Watkinson, "ISIS threatens Facebook founder Mark Zuckerberg and Twitter CEO Jack Dorsey in chilling video," *International Business Times*, February 25,2016, accessed March 2, 2016, http://www.ibtimes.co.uk/isis-threatens-facebook-founder-mark-zuckerberg-twitter-ceo-jack-dorsey-chilling-video-1545849.

disgruntled, and/or naïve around the world continue to resonate.[49] For Daesh and its domain of influence, social media is as compelling as any captured American tank or rocket launcher. By providing immediate access to other radicals, the social media space provides a virtual "echo chamber" in which the most extreme ideas and suggestions receive the most encouragement and support—instantaneously. [50]

Additionally, state adversaries of the United States—Russia, China, and Iran among others—are leveraging the power and extension of cyberspace to shape domestic and international environments.[51] Many of these nations and non-state actors possess a multitude of outstanding mathematicians, software writers, and media experts who, driven by intense ideologies or pure malice, are applying technical and cognitive understanding of cyberspace across the range of strategic thought in support of their political aims.[52] The fighting forces of many state and non-state actors are effectively navigating and exploiting activity in cyberspace with a deep appreciation of its potential to reshape warfare.[53] As the operational landscape continues to rapidly change, the US Army's need to study implications that the future has already challenged us with is a fateful imperative.

Beyond the recent Daesh example, consider the following hypotheticals – all of which are plausible and represent a mere fraction of the possibilities associated with cyberspace. How would the conventional Army respond to a known or unknown adversary of the United States that: (a) uses cyber technology to disrupt early warning radar systems within a theatre of operations; (b) implants a worm into

[49] Hisham Melhem, "Keeping Up With the Caliphate: An Islamic State for the Internet Age," *Foreign Affairs* 94, no. 6 (2015): 148-153.

[50] Tim Stevens and Peter R. Neumann, "Countering Online Radicalisation: A Strategy for Action," *Policy Report* of the The International Centre For The Study of Radicalization and Political Violence, March 16, 2009,12, https://cst.org.uk/docs/countering_online_radicalisation1.pdf.

[51] Thomas, 381-382.

[52] Thomas, 381.

[53] Johan, Sighholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies* 4, no.1 (2013): 32, accessed October 15, 2015, http://ojs.tsv.fi/index.php/jms/article/view/7609/pdf_1.

a DOD network that slowly corrupts GPS data on which military applications rely; (c) significantly degrades or disrupts Army command and control systems at home and/or abroad; (d) manipulates the social media feeds of US citizens to create fear and confusion across the country. Not only are the answers complex and unclear, they are not thoughtfully discussed – if at all – as part of the Army's current professional military education curriculum.

While we cannot forecast the future, the actors who invest most in understanding the range of potential impacts of cyber technology will be better suited to deal with the ambiguity and complexity of everyday life and the conduct of war in the twenty-first century. Efforts to project power throughout the world remains a top priority for the United States. As next-generation will-be nonstate terrorists and nation state adversaries are growing up with increasing use of computers and smart phones, the advent of attacks on critical infrastructure of magnitudes greater than those previously witnessed, are likely approaching in addition to a range of other unforeseen challenges associated with dependency on cyber technology.[54] In examining the rapid growth over time of the potential power and risks of cyber techno-social relations, the Army *must* prioritize and empower leaders at all levels of war to deepen its understanding of cyberspace and its impacts on war and warfare.[55]

Cyberspace and the Operational Artist

Thirty three years ago, in 1982, the year of the author's birth, there was no global Internet. Personal computers were in less than five percent of US households and they were slowly finding their way into the personal offices of the most senior of Army leaders. There were no magnetic resonance imaging (MRI) machines with which to assess the status of a soldier's injury, no fiber optic

[54] Sighholm, 32.

[55] Walter Issacson, "The Future of the Human Spirit in a World of Machines," May 14, 2015, (video of guest speaker for Smithsonian Magazine's The Future is Here Festival), accessed October 11, 2015, http://www.smithsonianmag.com/videos/category/future-is-here/future-is-here-festival-2015-walter-isaacson/#ooid=BwczB5dTrQqajwipRxK0OBxxcJxW0v7Z.

communications to send or receive operations orders instantaneously, no Global Positioning System (GPS) navigation to put steel on target with precision, and no way to imagine harvesting food with computer code.[56] Today, it would be difficult to find a soldier who did not have a mobile smart phone computer in his or her pocket with the capability to perform or provide instant information related to multiple tasks, impossible in 1982. To add additional context and perspective, Annie Jacobson writes, "By June 29, 2007, when Apple rereleased its first-generation iPhone, Americans could now carry in their pockets more technology than NASA had when it sent astronauts to the moon."[57] In the nine years since, the iPhone has more than followed Moore's Law, allowing capabilities such as virtual reality and control of internet-connected devices to be carried in one's pocket.[58]

One of the most challenging attributes of cyber technology is the speed of its evolution, its distortion of time, and its obliteration of space, recreating the shock that the Western world must have experienced with the first transatlantic telegraph messages, but on a near daily basis, often leaving insufficient time to understand, conceptualize, or exploit its effects.[59] As these ideas apply to war preparation, Army leaders and planners continually work to be fluent in the language of operational art, defined in ADRP 3-0 as "the pursuit of strategic objectives, in whole or in part, through the arrangement of tactical actions in time, space, and purpose."[60] Army doctrine further states that this approach enables commanders and staffs to use skill, knowledge, experience, and judgment to overcome the ambiguity and

---

[56] Caleb Harper, "This Computer Will Grow Your Food in the Future," *TED Talks*, accessed January 20, 2016, http://www.ted.com/talks/caleb_harper_this_computer_will_grow_your_food_in_the_future.

[57] Annie Jacobson, *The Pentagon's Brain: An Uncensored History of DARPA, America's Top-Secret Military Research Agency* (New York, NY: Little, Brown & Company, 2015), 412.

[58] Jonny Evans, "Is the iPhone evolving faster than Moores Law?" *Computerworld*, August 27, 2010, accessed May 6, 2016, http://www.computerworld.com/article/2468951/mobile-apps/is-the-iphone-evolving-faster-than-moore-s-law-.html.

[59] Rochlin, 205.

[60] Army Doctrinal Reference Publication 3-0.

intricacies of a complex, ever changing, and uncertain operational environment to gain a more fluent understanding of problems.[61]As the core and essence of operational art, the dimensions of time and space define the execution and narratives of all wars and are examined in the work's next section.

The First Condition of Adequacy: Accounting for Time and Space in the Contemporary Operating Environment

This section examines multi-disciplined arguments to address the first condition of adequacy and the first research question, which asks how the fundamental concepts of time and space relate to cyberspace and current executions of operational art. The work does so through discussion of concepts, of and related, to space and time in military and societal contexts throughout history. It also presents multiple vignettes that demonstrate how cyberspace challenges contemporary conceptions as compared to representations within core Army doctrine. The author illustrates the value to be derived from increased study of the fifth domain in preparing for the inherent ambiguity of war.[62]

Philosophy is an academic discipline that attempts to understand reality and answer fundamental questions about knowledge, life, morality, and human nature. Philosopher John Campbell, describing the purpose of philosophy, asserts, "It helps break down, describe, and assesses moves we ordinarily make at great speed…It then becomes evident that alternatives are possible."[63] With that context in mind, philosophy's relationship to framing the operational environment and the execution operational art is of value to the military planner.

---

[61] Ibid.

[62] Larry D. Welch, "Cyberspace – The Fifth Operational Domain," Institute for Defense Analysis, Research Notes (2011), accessed March 16, 2016, https://www.ida.org/~/media/Corporate/Files /Publications /ResearchNotes /RN2011/2011%20 Cyberspace %20-%20The %20Fifth%20Operational%20Domain.pdf.

[63] Harvard University Department of Philosophy, accessed March 15, 2016, http://philosophy.fas.harvard.edu/why-study-philosophy.

The philosophical concepts of time and space are fundamental to our understanding of human existence. Increasingly, activity influenced by cyber technology is filtering into this understanding. Unlike many other characteristics of the young cyber domain, the concepts of time and space have been subjects of evaluation throughout recorded history. Newton's views on space and time dominated physics and philosophical thought from the 17th Century until the advent of the theory of relativity in the twentieth century. In the Newtonian perspective, *space* is distinct from body and *time* passes uniformly without regard to whether anything happens in the world.[64]

Einstein's theory of special relativity, supported by a century of work by other physicists, however, has shown that these notions may be subjective. In the age of relativity, wherein society experiences time as Einstein imagined it, time contracts and expands relative to the velocities of observers. The reality of nature according to quantum theory, therefore, is a realm of possibilities and probabilities.[65] It follows that as vivid as our experience of the passage of time in space may appear to us, this appearance may not reflect a fundamental aspect of reality. While the human design and use of cyber technologies creates cyberspace, such space is not metric; most of the ready-made constructs, like the topology of space or even the relativistic time– space continuum, are too imprecise for a true appreciation for the complexity of the cyber domain.[66]

In his work on International Conflict and Cyberspace Superiority: Theory and Practice, William D. Bryant writes that cyberspace is difficult to grasp intuitively because we cannot experience it directly with our senses. "We can stand on the land, dive into the water, and see aircraft or satellites with our eyes." The intimate connection between cyberspace and physical space also represents a fundamental

---

[64] Staff of the Stanford Encyclopedia of Philosophy, "Newton's Views on Space, Time and Motion," last modified August 22, 2011, accessed April 10, 2016, http://plato.stanford.edu /entries/newton-stm/.

[65] Everett Carl Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005), 98.

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

difference between them, as physical space depends on nothing at all.[67] We have to rely on screens or representations to "see" it, but we are not directly experiencing cyberspace. According to Professor Chris Demchak, "Cyberspace is hard to see physically in any case, but especially so now as it is deeply embedded in normal societal functions."[68]

Yet despite our inability to see, touch, or measure all properties of the domain, cyberspace has become fundamentally important to the everyday working of society and critical to all military operations. As a result, the Army writ large is compelled to reconsider its understanding of time and space in in a world in which cyber technology is deeply and totally embedded and in which the institution is now dependent. To make the evolution in conceptualizing time and space feel more tangible for the reader, the author now compares a work of contemporary art and two historic, globally recognized boating tragedies that occurred approximately one hundred years apart.

Over one hundred years ago, the failure of the communications equipment aboard the Titanic, significantly complicated rescue efforts. Although the Titanic's owners boasted that the ship was the most modern of its day, the radio system installed in the weeks before the disaster was already obsolete.[69] The actual confirmation of the sinking took three days to reach land with the facts associated with the tragedy unclear to the world until the survivors reached New York.[70] Figure 1 is the work of a French artist satirically depicting contemporary society's response if Titanic were to sink in 2015. Victims of the

---

[67] Rebecca Bryant, "What Kind of Space is Cyberspace?" *Minerva - An Internet Journal of Philosophy* 5, (2001), http://www.minerva.mic.ul.ie//vol5/cyberspace.html.

[68] Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA : University of Georgia Press, 2011), 176.

[69] Bill Kovarik, "The Radio and The Titanic," accessed April 5, 2016, http://www.environmentalhistory.org/revcomm/features/radio-and-the-titanic/.

[70] Ibid.

disaster are shown recording the tragedy as it unfolds, filming and taking selfies as they tread for their lives.[71]

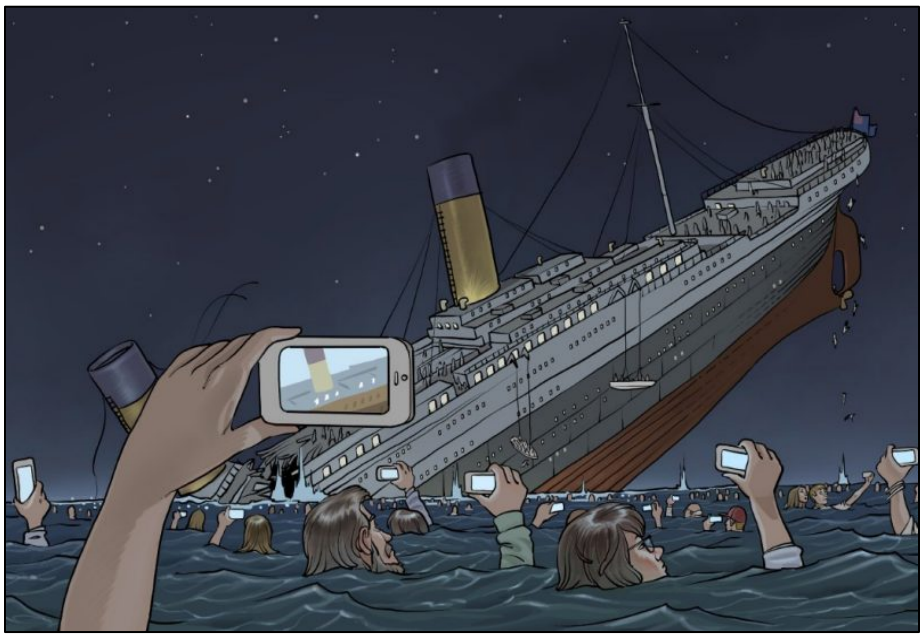

Figure 1. If the Titanic sank in 2015.

Source: Cartoonist Pierre Brignaud, as part of the International Visual Arts Contest Just for Laughs 2015, accessed January 15, 2016, http://www.oeilregional.com/opinion/2015/7/27/3e-place-pour-pierre-brignaud.html.

If his artistic visualization seems improbable, one only has to recall the tragic passing of 295 individuals aboard a South Korean Ferry in 2014. Video clips from recovered cell phones show teenagers anxiously referring to the sinking ferry as their "Titanic." Not fully aware of the seriousness of their peril, the teens wonder if they will make the news and discuss posting about the excitement on Facebook.[72]

[71] Pierre Brignaud, as part of the International Visual Arts Contest Just for Laughs 2015, accessed January 15, 2016, http://www.oeilregional.com/opinion/2015/7/27/3e-place-pour-pierre-brignaud.html; A selfie is defined by Websters as a digital image of oneself taken by oneself usually for posting on social media.

[72] Patrick Gerrity, “South Korea Ferry: Heartbreaking Video Shows Last Minutes Aboard,” May 1, 2014, accessed January 15, 2016, http://www.nbcnews.com/storyline/south-korea-ferry-disaster/south-korea-ferry-heartbreaking-video-shows-last-minutes-aboard-n94876.

If a similar event were to happen today, in 2016, Facebook, among other popular social media platforms, now provides the potential for a tragedy such as this to be recorded live and broadcast globally among millions of subscribers.[73] Throughout the range of life experiences on Earth, one culture's totally normal practice may be taboo in another and lead to potentially unprecedented cultural conflicts and opportunities. While this opens positive and empowering new vistas for those with the ability and interest in making these live connections, the potential broadcast of unsavory material is also real. Twitter's launch of their live streaming feature has captured a range of activity in real time from violence on the streets of Jerusalem to video of the Paris attacks, literally as they unfolded.[74]

Cyber technology today allows for the transcendence of perceptions of fixed time and space. Postmodern theorist Paul Virilio suggests in *Pure War* that all history was written in local space and time.[75] For example, time and space for Titanic passengers in the North Atlantic's icy waters was distinct from the time and space of their family members residing in New York City or elsewhere. In the twenty-first century, physical space includes all the potential of virtual space with history synchronized to world time. Cyber technology as represented in this example of artwork and in consideration of instant streaming social media applications allows for the synthesis of experiences in totally disparate physical

[73] Julia Greenberg, "Facebook's Plan to Stop People From Livestreaming Sex? You," *Wired Magazine*, April 8, 2016, accessed April 9, 2016, http://www.wired.com /2016/04/facebooks-plan-stop-people-livestreaming-sex/.

[74] Posts praising and encouraging attacks on Israelis have emerged on YouTube and Facebook, while Twitter hashtags including "Jerusalem Intifada" or "Intifada of the Knives" are gaining traction among Palestinians. See "Is Palestinian-Israeli violence being driven by social media?" BBC News, October 22, 2015, accessed January 15,2016, http://www.bbc.com /news/world-middle-east-34513693.

[75] Paul Virilio and Sylvère Lotringer, *Pure War: Twenty-Five Years Later*, new and updated ed. (Los Angeles: Semiotext(e), 2008), 205. For more on postmodernism, See Mary Jo Hatch's Work on Organization Theory. She explains that in postmodernist thinking, knowledge cannot be an accurate account of truth because meaning cannot be fixed; there is no independent reality; there are no facts, only interpretations; knowledge is a power play.

locations simultaneously. In its man-made and hyper-evolving configurations, cyberspace is at once chronically instant, everywhere and nowhere.[76]

This capability creates vast new challenges in leadership and operational planning. How does this capability square, for example, with the presumption of innocence when a soldier is captured on film committing a war crime? What are the implications for soldiers operating in environments where increasing amounts of the population have access to this technology? Can acceptable constraints be placed on soldiers to minimize the potential for misuse or does the prohibition of cyber technologies decrease situational awareness and actually promote inappropriate activity in cyberspace?

The newness of this particular live streaming technology and the inability to forecast how the capability will effect society or the military makes understanding its implications extremely difficult. However, to ignore the potential opportunities and challenges for the operational artist is troublesome given growing evidence that cyber technologies *are* affecting and perhaps transforming, how people interact with each other, with data, and with their surroundings. Specific examples of the Army's inadequate conceptualization of cyberspace will be addressed in the paragraphs that follow.

Fixing of Space

In the study of war over many centuries, it is evident that social, political, and technological factors have influenced, or in other words, "fixed" the determination of the space in which humans conduct battle. For example, the centralized control of state resources in the early Modern period contributed to the increased mobilization of manpower and enlarged the scope of the battlefield, while setting conditions for the modern military profession.[77] In the nineteenth century, the increasing scale of

[76] Virlio, 205.

[77] John Andreas Olsen and Martin van Crevald, eds., "Conclusion," in *The Evolution of Operational Art: From Napoleon to the Present* (Oxford: Oxford University Press, 2011), 222-5; see also Michael D. Kruause and R.Cody Phillips, eds., *Historical Perspectives of the Operational Art* (Washington, DC: Center of Military History, 2007).

land warfare, necessitated by the increasing lethality of the battlefield, forced an increase the physical space over which single engagements tended to occur.[78] Military efforts began to require greater synchronization in order to achieve strategic aims and drove the formation of tactical actions into campaign frameworks.[79]

Twenty-first century characterizations of space are markedly different from those of previous eras. From the storage of information to social media platforms instantly amplifying global communication, space in cyberspace includes algorithms of bits and bytes that have the ability to rapidly replicate, iterate, and mutate.[80] Until recently, territorial boundaries were clear, with mountains, rivers, and walls as physical barriers between adversaries. For example, during the Cold War, the United States and the North Atlantic Treaty Organization (NATO) prepared for an allied response to a Soviet tank invasion along the Fulda Gap between East and West Germany. In today's environment, an adversarial hacker in Russia has an entirely different destructive capability in his mind and in his arsenal. Simply with access to a modem or smart phone, from anywhere in the world, the Russian government-sponsored hacker has the potential to deploy cyber code programmed for deliberate effects against a networked target anywhere advantageous to aim accomplishment.[81] Whether or when that adversary crossed an international boundary to do so is difficult to determine, but, more importantly, it is irrelevant.

The current mindset of the Army predominately leaves the charge of understanding cyberspace to those trained to serve in cyber or military intelligence positions. Both ADRP 3-0, *Unified Land Operations (ULO)* and ADRP 3-90, *Offense and Defense*, fail to appropriately account for the influence

[78] Olsen and van Crevald, 222-5.

[79] Ibid.

[80] A bit is the smallest unit of data and it can be coded as being "on" or "off" or, equivalently, as a 0 or a 1. One byte is the grouping of eight bits, e.g., 01011010. In the writing of code, one byte can store one letter.

[81] Segal, 12.

of cyber technologies on physical events in time and space. Despite the potential of cyberspace to significantly affect all operations in physical realm, its potential impacts are insufficiently addressed. In the Army's doctrinal reference publication on offense and defense, the word "cyber" is found only four times in its 124 pages of "guidance in the form of combat-tested concepts and ideas modified to exploit Army and joint offensive and defensive tasks."[82] Without appropriate emphasis in core doctrine, both in the field and in the classroom, this cultural mind shift will be long in the making.

Time and Decision Time

Standardized time according to which most societies now function is an invention of the mid-nineteenth century.[83] It was invented for the efficiency of railroad operation and coincided with the Industrial Revolution. Prior to the institutionalization of standard time, clocks were set using widely varying local meridians or local mean times.[84] The timeless nature of the Internet has coincided with globalization. As part of his overall argument that time is a more significant variable than space in military planning, Robert Leonhard argues in *Fighting by Minutes* that the advantage of time has been crucial to success at every level in war throughout history. He further suggests that, more than with any other technological advance, changes in communications often mandate changes in tactical doctrine and that the full incorporation of new technologies will change the perception of the very meaning of victory or defeat in battle.[85]

[82] Army Doctrine Reference Publication (ADRP) 3-90, *Offense and Defense* (Washington, DC: Government Printing Office, 2012).

[83] D'erasmo, "Living on Internet Time."

[84] Ibid.

[85] Robert R. Leonhard, *Fighting by Minutes: Time and the Art of War* (Westport, CT: Praeger Publishers, 1994), 124.

In the period of the Napoleonic Wars, decisions that ultimately led to battle were measured in days or weeks before the first shot was fired.[86] In World War One, commitment time to start the war was measured in days, where commitment for decisions in combat was often measured in hours. Plans defined the actions of actors and there was little way to alter the course of the battle.[87] This trend in the shortening of time horizons for decision making has continued, and the operational environment today is "as short in decision time as it is high in information flows."[88] As part of decisions made within or influenced by cyber technology, the time from detection to commitment is measured in fractions of seconds and, in some cases, is not made by a human.

The ability for events to happen nearly simultaneously within cyberspace has potential impacts in physical space. Consider the instantaneous nature of the synchronized collection of millions of data points from networked people and things with unlimited regard to physical location. An Internet-based platform website is not merely a point in space, but a space-time synthesis which we refer to in locational terms. [89] In April 2013, the Syrian Electronic Army (SEA) hacked the Twitter account of the Associated Press by sending malware through a "phishing" email.[90] The software allowed the hackers the ability to send an erroneous tweet about bomb attacks in the White House and the injury of President Obama. Within seconds, the Dow Jones Industrial Average plunged 146 points, near instantly erased 136 billion dollars in market value. The market bounced back almost as quickly as it fell, but the event demonstrated

---

[86] Rochlin, 204-205.

[87] Ibid, 205. The innovation and mission command employed by the Germans ultimately broke this cycle of cognitive distortion.

[88] Ibid, 204.

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

[90] Nicole Perlroth, "No Joke: Syrians Hack the The Onion," Bits (blog), *New York Times*, May 6, 2013, accessed March 24, 2016, http://bits.blogs.nytimes.com/2013/05/06/no-joke-syrians-hack-the-onion/?_r=0.

the speed at which complex systems could be destabilized and trust in information systems undermined at all levels of governance.[91] All indications suggest that the increase of ubiquitous cyber technologies into our lives will continue and every element of combat will be effected, thus, proper conception of the operational environment must be made adequate as cyber technologies are far more significant than the capabilities they bear.

Virtual Space and War

The compression of time and space that characterizes activity in cyberspace includes the experiences of virtual reality (VR). VR is a fabricated experience made possible by cyber technologies that humans perceive to be so real as to be indistinguishable from the "really real" world.[92] Crucially for practical effects, once persons believe that a digital experience is real, their experiences in the physical realm can be more easily manipulated.[93] The US Army already employs virtual reality in a variety of ways and has for over two decades.[94]

In his experiences observing war simulations at the National Training Center, Professor Der Derian writes, in *Virtuous War*, "New technologies of imitation and simulation as well as surveillance and speed…collapsed the geographical distance, chronological duration, the gap itself between the reality and virtuality of war."[95] Arguably, since the Gulf War of 1991, this blurring of real war and virtual war has

---

[91] Segal, 17.

[92] Jim Blascovich and Jeremy Bailenson, *Infinite Reality: Avatars, Eternal Life, New Worlds and the Dawn of the Virtual Revolution* (New York: HarperCollins, 2011),15.

[93] Matthias Mccoy-Thompson, "Virtue and the Virtual—The Moral Implications of Virtual Reality," A Medium Corporation, February 29, 2016, accessed March 2, 2016, https://medium.com/the-metaverse-muse/virtue-and-the-virtual-7092af8b34ec#.lz405mmbt.

[94] David L Neyland, *Virtual Combat: A Guide to Distributed Interactive Simulation* (Mechanicsburg, PA: Stackpole Books, 1997), 1.

[95] Der Derian, *Virtuous War: Mapping the military-industrial-media-entertainment network* 2nd ed. (New York: Routledge, 2009), 11.

existed. The Gulf War, which was broadcast in near real time, distorted the conceptual division between war and peace. Although Western viewers watching from the comfort of their living rooms saw "smart bombs exploding, footage of disoriented Iraqi troops fleeing and being bombarded were largely hidden from the television audience."[96]

The implications on future policy making or perceptions by society in seeing the military as an inanimate tool whose work in some cases is indistinguishable from a video game is not emphasized in Army policy, doctrine or as part of professional military education.[97] This is a concern given the ease in which real and virtual training environments blend. Instead, Army simulations are highlighted for their value in providing realistic simulated warfighting experiences and reducing overall training costs.[98] Unlike actual war or dangerous training environments on actual terra firma, the cost of mistake or misfortune is not death.[99]

In consideration of this blending, many questions emerge. Does the blurring of virtual and real environments make decision making in the latter easier or more difficult over time? Even if virtual practice does improve comfort with actions or decision-making, what does the increased reliance on this disembodied experience signify for sustained long-term combat where an individual cannot simply power off the experience? The Army must work to understand the implications of life within and between these

---

[96] Chris H. Gray, *Kuwait 1991: A Postmodern War, 1991*, Chapter 1, accessed April 9, 2016, http://www.guilford.com/excerpts/grayEX.html.

[97] Daniel T. Zimmer, *Programmatic Integration of Cyber into The Institutional Domain of Leader Development*, (Master of Military Art and Science Thesis, Command and General Staff College, 2015). The author conducted a cross case comparative analysis to identify what cyber leader development the Army's Training and Doctrine Command is currently implementing within Army learning institutions. The author compares that emerging program to historical cases of other leader development programs created in response to technologies that changed how the Army developed its leaders in the past.

[98] Jane Benson, "Virtual Reality Dome Impact of Real-Life Scenarios on Cognitive Abilities," The Official Homepage of the United States Army, February 24, 2016, accessed 7 March, 2016, http://www.army.mil/article/162899/Virtual_reality_dome_impact_of_real_life_scenarios_on_cognitive_abilities/.

[99] Der Derian, 11.

two domains and the effects they have on each other. This requires thoughtful examination from both strategic and cultural perspectives, especially given projections of the Army's employment of virtual reality training. [100] How cyber technologies alter space and time to create virtual space must be included in describing current operational environments affected by cyberspace in order to be adequate.

The twentieth century philosopher Peter Lamborn Wilson (alias Haikem Bey,) proposed the concept of *hyperreal* war which he suggests began in Vietnam with the involvement of television and reached full exposure in the Gulf War of 1991. Bey distinguishes three types of war: ancient and largely ceremonial ritual brawls, increasingly technical war that "occurred at least through World War II," and the third, hyperreal war, conducted in the forms of images and internalized in the mind.[101] He noted, "[I]n the first the body is risked; in the second, the body is sacrificed; in the third the body has disappeared," suggesting that today, there are elements of war whereby, "[T]he body disappears as an object of vision, although of course, the body itself does still exist and is being subjected to the same sacrifices that always existed."[102]

In 2002, the joint military training event named "Millennium Challenge" blended reality and video gaming to simulate the United States fighting a Middle Eastern adversary, presumably Saddam Hussein's Iraq. As chronicled in Malcolm Gladwell's *Blink*, and acknowledged by the military in a final 752-page report on the event, the exercise was recalibrated after the red team's success using asymmetric tactics overwhelmed the blue force's systems and planning. For example, the red team commander destroyed sixteen American ships with a notional fusillade of cruise missiles and had the exercise been a real war, "twenty thousand American servicemen and women would have been killed before their own

[100] Jane Benson, "Virtual Reality Dome Impact."

[101] Jonathan Taylor, "The Emerging Geographies of Virtual Worlds," *Geographical Review* 87, no.2 (1997), 192-192, accessed February 29, 2016, http://www.jstor.org/stable/216004.

[102] Ibid.

army had even fired a shot."[103] Rather than requiring that the joint staff work through the complexity posed by the red team as part of the scenario, the variables of the scenario were recalibrated to accommodate the victory of the joint plan.[104] Perhaps of most concern, the simulation of success supported the political aims of those wishing to turn their attention to the real Persian Gulf.

The 2015 DoD operational test and evaluation (DOT&E) report recently examined the role of cyber activities as part of thirteen different training exercises. It concluded that most military exercises do not appropriately account for cyberspace. Furthermore, the report stated that "exercise authorities seldom permitted cyber attacks from being conducted to the full extent that an advanced adversary would likely employ during conflict."[105] In both cases, the military's ability and tendency to want to control war and manipulate virtual war conditions in the favor of the friendly force are largely unconstructive for the purposes of military strategy.

Given the increase in use of these cyber technologies, one would think, at a minimum, that the Army's professional military education programs would provide multiple training opportunities for the complexities and confusion of the real world to inform notional war scenarios. However, adjustments in favor of friendly forces often remains the fact in planning and wargaming.[106] Although there are indications to suggest value in simulations associated with the conduct of war, evidence, such as suggested herein, also illustrates potential danger of leveraging these virtual spaces to support illusions of

[103] Ibid, 110.

[104] Malcom Gladwell, *Blink: The Power of Thinking Without Thinking* (New York: Little Brown and Company, 2005), 99-145.

[105] Jared Serbu, "Pentagon Report Says Most Military Exercises Don't Account for Cyber Threats," *Federal News Radio*, February 2, 2016, accessed February 11, 2016, http:federalnewsradio.com /defense/ 2016/02/pentagon-report-says-military-exercises-don't-account-for-cyber-threats.

[106] This is based in part on the authors experience while assigned at the Command and General Staff College and School of Advanced Military Studies, and Army service on active duty since 2004.

control, both in breeding false senses of military confidence and as a way to manipulate public and governmental support favoring a particular strategic political aim.

This virtual expression of war continues today. One example outside of the training realm is the current social media coverage of coalition efforts against Daesh. The Combined Joint Task Force Operation Inherent Resolve (CJTF-OIR) posts information on a US government-hosted website in addition to a variety of social media platforms.[107] Among many brief written updates and articles, dozens of videos, called "Strike Updates," are posted that visually depict targeted destruction of assessed enemy command and control elements and support infrastructure.[108] Research suggesting the relative impact of CJTF-OIR's social media campaign was not found. Numerous open source reports and opinions regarding the efficacy of the air strike campaign however are plentiful. This supports the early suggestion that much work remains to be achieved in understanding the social implications of cyberspace.

The incorporeal experience of unique interactions in and through cyberspace and its fundamentally complex nature makes comprehension of it and all related ideas challenging. However, these ideas and examples suggested here make apparent that beyond understanding cyber capabilities, the Army must thoughtfully account for a new, global understanding of time and an appreciation of space in its virtual forms as part of an adequate comprehension of cyberspace and the operational environment.

Broadening the Army's Conception of Time, Space and Cyberspace

The military's struggle against the inevitable chaos of environments and the spontaneous activity that occurs within it is constant.[109] This idea is supported by the Department of Defense's Third Offset Strategy and the increasing investments by the Defense Advanced Research Project Agency (DARPA) in

[107] Combined Joint Task Force, *Combined Joint Task Force Operation Inherent Resolve* (video), accessed 7 April, 2015, http://www.inherentresolve.mil/Video.

[108] Ibid.

[109] Virlio, 96.

cyber technologies, specifically, deep learning computers, artificial intelligence, and virtual reality among other potentially game changing technologies. [110]

At present, very few of these new dimensional understandings are reflected in Army operations doctrine outside of cyber and information operation-specific doctrinal references. The preponderance of Army doctrine derives understanding of space and time largely from four-dimensional thinking based upon Newtonian physics, linear dynamics, proportionality, synchronized processes, and reductionist principles.[111] The Department of Defense elevated cyber to a domain status in 2011 to direct the treatment of cyberspace as "an operational domain to organize, train, and equip so DOD can take full advantage of cyberspace's potential."[112] In so doing, it "unintentionally forced the discussion away from the properties of cyberspace and its impacts on society and modern warfare," writes Martin C. Libicki in his essay, "Cyberspace Is Not a Warfighting Domain.[113]" Libicki contends that the effort to make cyberspace a fifth domain misrepresents the problem thereby leading "strategists and operators to presumptions or conclusions that are not derived from observation and experiences." He further contends that by calling cyberspace a domain, but a really different one, begs the question of what purpose is served by calling cyberspace a domain to begin with.[114]

---

[110] Jacobson, 451; Bob Work, "The Third US Offset Strategy and its Implications for Partners and Allies" Deputy Secretary of Defense Speech, January 28, 2015, accessed December 17, 2015, http://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies.

[111] Robert J. Bunker and Charles "Sid" Heal. *Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and War* (Bloomington: iUniverse, 2014).

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

[113] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 325-340.

[114] Ibid.

According to Army Unified Land Operations, time is assessed as an operational and mission variable. As an operational variable, time describes the timing and duration of activities, events, or conditions within an operational environment and also how such timing and duration are perceived by various actors in the operational environment.[115] References to the cultural perception of time, information offset, tactical exploitation of time and key dates, time periods, or events are listed within the doctrine, but no context including references to cyberspace are provided. As a mission variable, doctrine suggests that commanders assess time as the time available for planning, preparing, and executing tasks and operations. This includes the time required to assemble, deploy, and maneuver units in relationship to the enemy and conditions.[116] A majority of references to space is combined with the variable of time. Time and space are primary components of operational art; with time as critical to the generation of maneuver space. There is little, if any, specific recognition of the effects that cyber technologies bear on time or space in this and other core doctrinal references.

The Army's understanding of cyberspace is currently centered on the means and not on an overarching strategic frame.[117] The task of the operational artist however, is to temporally integrate and spatially distribute operations into one coherent whole.[118] Clausewitz emphasized the purpose of war as compelling the enemy to do your will.[119] Sun Tzu argued that the best form of warfare is the one in which the enemy is seized without a fight.[120] The strategic application of cyberspace iterates the essence of both

---

[115] Army Doctrine Reference Publication (ADRP) 5-0, *The Operations Process* (Washington, DC: Government Printing Office, 2012).

[116] Ibid.

[117] Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," accessed April 6, 2016, https://ccdcoe.org/publications/books/VirtualBattlefield.pdf.

[118] James Schnieder, "The Loose Marble – and Origins of Operational Art," Parameters, Vol 19, (March 1989), 85-99.

[119] Von Clausewitz, Book I, 75.

[120] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford University Press, 1963).

of these revered military theorists. Cyberspace creates potentials to paralyze an enemy strategically to achieve desired ends with little or no application of physical force. There have been many efforts to find lines of similarity between more conventional armed conflicts and conflict in cyberspace, but these arguments arguably degrade the strategic aspect of cyber warfare to mere tactical cyber offensive or defensive activities.

Organization and reorganization of the Army in its development of cyber branch and in training cyber warriors has done little to address basic questions about military strategy. Traditional models of understanding have limited application in adequately describing cyberspace. Johnson-Freese argues that once a weapon or a domain gets its own bureaucracy, inertia becomes an organizations guiding strategic principle.[121] Army leaders across all branches must have the courage to challenge foundational assumptions of time and space to gain a deep and broad understanding of the operational environment of the twenty first century. To affect change, the perception of a majority of military practitioners and the The way in which the Army views the significance of cyberspace must change.[122] The Army's present conception of time and space with effects on physical space currently fail to meet the first condition of adequacy proposed at the start of this monograph. As a first step, core Army doctrine and professional military education training opportunities must account for cyberspace in representations of the contemporary operational environment or the Army will continually cede the strategic advantage to adversaries who do.

The Second Condition of Adequacy: Emphasis on Techno-Social Relations

This section will cover three ideas related to the second condition of adequacy. The second condition of adequacy requires proper weighting of the relationship between cyber technology and human

[121] Johnson-Freese, "Domains, Budgets and Bureaucracies: Nukes, Space & Now – Cyber."

[122] Patricia Frost and Matthew Hutchison, "The Top 10 Questions for Commanders to Ask About Cyber Security," *Small Wars Journal*, December 8, 2015, accessed February 11, 2016, http://smallwarsjournal.com/jrnl.art/top-10-questions-for-commanders-to-ask-about-cybersecurity.

behavior from both friendly and adversarial perspectives. First, how individuals form identities in cyberspace and the effect these individual approaches have on power dynamics and the roles actors play in physical space is explored. Second, generational differences as related to these concepts are addressed. Finally, the author addresses some potential implications of the DoD's Third Offset Strategy for the Army. The overall intent of this section is to illustrate the importance of understanding emergent techno-social dynamics in the development of military strategy.

The effects of cyber technology on humans and on conflict have yet to be analyzed systematically and programmatically in conventional military circles. The central role of humans in war has always been an important, if not the most important, consideration in understanding conflict. Humans increasingly interface with cyber technology. Understanding that the resulting system can provide an alternative environment for human interaction is important to gain full appreciation of the risks and potential of cyberspace in informing strategy. The Internet is a sufficient example of how many-to-many communication tools perform as instruments to facilitate shifts in political power.[123] The ability to communicate words, images, and sounds globally heightens the ability to persuade, inform, witness, debate, and discuss on an unprecedented scale and at an unprecedented rate. Additionally, the power to slander, propagandize, engage in misinformation and/or disinformation is no longer the sole province of institutions or wealthy individuals who own or control traditional media sources. [124]

As a result, today's operational environment must factor the potential power of an individual or group to shape the overall narrative of a conflict with potential effect on individual and group behavior at

[123] Maura Conway, "Terrorism and IT: Cyberterrorism and Terrorist Organizations Online" (paper presented at the International Studies Association (ISA) Annual International Convention, Portland, Oregon, February 25 – March 1, 2003),1-2, accessed March 15, 2016, http://www.doras.dcu.ie/502/2/terrorism_it_2003.doc.

[124] Ibid., 2.

scale.[125] Similar to the challenges of conceptualizing time and space and virtual space recognized in relation to the first condition of adequacy, the intangible nature of social identity makes it tempting to minimize in significance. What follows are illustrations as to why understanding identity and the concept of legitimate virtual identities in the twenty-first century matter to the Army practitioner in adequately conceptualizing the potential of cyberspace.

Real and Virtual Identity: What's in a name?

Cyberspace is created by humans for human purposes. Turkle writes "We make our technologies and they, in turn, make and shape us."[126] Without human users, cyberspace would deteriorate and eventually fail to exist. Unless or until something else takes over the maintenance and development of cyber infrastructure and its content, the human remains an important part of the potential of cyberspace. Human identity is a unique creation of self through societal forces, interpersonal relationships, and geographical, political, and cultural motivations.[127] Sociologist Erik Erikson formulated that a healthy identity is a multifaceted but ultimately coherent sense of self that is personally satisfying while at the same time being recognized and affirmed by the surrounding community.[128] When individuals invest in online experiences, they belong to different communities, practice different norms and values and are provided the opportunity to perform various identities in movement from one context and space to

[125] Paul Scharre, *Uncertain Ground : Emerging Challenges in Land Warfare* (Washington, DC: Center for a New American Security, 2015), accessed on December 22, 2015, http://www.cnas.org/search/site/Uncertain%20Ground%20%3A%20Emerging%20Challenges%20in%20Land%20Warfare.

[126] Turkle, 263.

[127] N. B. Ellison and D. Boyd, *Sociality through Social Network Sites,* in *The Oxford Handbook of Internet Studies* (Oxford, UK: Oxford University Press, 2013), 151-172.

[128] Erik H. Erikson, *Identity: Youth and Crises* (New York: W.W. Norton, 1968).

another.[129] Lacking visible bodies, self-representation in online spaces, sometimes in the construction of an avatar, offers participants many possibilities to create a representation of how they hope to be identified within a given context.[130] Friendships are formed, information is gathered, and impressions are made in cyberspace with potential impact on the behavior of individuals and groups in physical space.

Published in 1966, *The Social Construction of Reality* by Peter L. Bergman and Thomas Luckman constructs a sociological analysis of "knowledge that guides conduct in everyday life."[131] They clarify their definition of reality as that which is understood by the common sense of ordinary members of society.[132] The world today, connected and communicated through cyber technology, serves as a primary means for self-expression and identity formation. In some contexts, an online identity is clearly and directly linked to an offline presence. For instance, online dating profiles represent a person who is, seemingly, available for making offline connections.[133] In other contexts, the association to or the expectation of an offline presence is less important. Nevertheless, in all cases, making oneself visible to others online requires the presentation of a digital identity. There are over three billion people on earth today that have some form of digital footprint.[134]

In comparison to social groups formed in physical space, group interests online can be generated and shared with millions of people regardless of actual localization. Much like the blur of war discussed

---

[129] Howard Gardner and Katie Davis, *The App Generation: How Today's Youth Navigate Identity, Intimacy and Imagination in a Digital World* (New Haven. CT: Yale University Press, 2013), 60.

[130] "Avatar" is a word used for the image that a person chooses as his or her "embodiment" in an electronic medium.

[131] Peter L. Berger and Thomas Luckman, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (New York: Random House, 1966), 19.

[132] Ibid 19; As John Searle has pointed out, the reality referred to is the social interpretation and meaning of artifacts and events, not their observer-independent existence. John. R. Searle, *The Construction of Social Reality* (New York: Simon & Schuster, 1995).

[133] Ellison and Boyd, 151-172.

[134] A digital footprint is the data that's left behind whenever you use a digital service.

previously, the *social* distinctions between the real world and the mediated virtual world are also increasingly unclear. While socialization in cyberspace adds a new variable to the theory of social construction of reality, identity and reality formation still remain dependent on social and cultural influences. Experiences in physical realms continue to contribute to the understanding of self and the institutions by which individuals shape and conform.[135] As humans are the creators of the virtual domain, an interesting feedback loop develops in the sense that identity is both formed and shaped by virtual life experiences. Returning back to Berger and Luckman, if one agrees that there is no such thing as reality independent of its social construction and the way it is perceived and shaped by socialized agents, then increasing time spent, relationships forged, and experiences created online have a structuring effect on the physical life experiences of individuals and groups.

Consider the unprecedented ability of Daesh to recruit fighters purposed toward the effort to legitimize its declared caliphate. They have an incredibly robust online recruitment strategy that tends to use video of images rather than text, takes full advantage of the linguistic skills of members across the world, and makes good use of video gaming and music—all with powerful resonance on youth culture.[136] Daesh creates a fantasy initially realized in virtual reality. Its ideological call to action is pervasive and influential. [137] Energy is employed not only to recruit foot soldiers, but also to enlist technically proficient and talented users of social media to sustain the recruitment processes. Online recruitment is one of the organizations most prioritized and supported operations because they understand the ability to recruit as a strategic element of their campaign against the West.[138]

---

[135] Turkle, 11.

[136] Scott Gates and Sukyana Podder, "Social Media, Recruitment, Allegiance and the Islamic State," *Perspectives on Terrorism* 9, no. 4 (2015), accessed April 3, 2016, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/446/html.

[137] Hisham Melhem, "Keeping Up With the Caliphate: An Islamic State for the Internet Age," *Foreign Affairs*, November/December (2015), 148-153.

[138] Ibid.

Another current example is found in the experience of US soldiers. Every aspect of a soldier's daily life is affected by increasing dependence on cyber technologies. Firsthand accounts of how differences in non-battle time communication and socialization have manifest in combat performance are increasingly common. In one such provocative illustration captured in a New York Times article, "From Army of One to Band of Tweeters," Major John Spencer remarks on the cohesion of his troops both on and off the battlefield when serving in Iraq in 2003 and again in 2008.[139] He observes frequent and personal communication between his soldiers and their ability to work together under stress, remarkable.[140] Five years later, and complemented by upgrades in cyber technology, the officer recalls a stark change in "the soldiers' individuality in battle," especially among the youngest troops. He observed an increase in the frequency of arguments over unit decisions and he characterized communications as more transactional as opposed to the friendly banter he was accustomed to on previous deployments.[141] His experience is not uncommon. The author had many conversations with fellow officers over the past two years regarding similar observations. In one such conversation, an Army military police officer and fellow SAMS student shared her frustrations. During convoy operations, she observed soldiers with more interest in developing a most efficient battle drill to charge their smart phones than concern in executing preventive maintenance checks and services (PMCS) on their Humvees.

Conventional wisdom claims that soldiers fight for each other. Since World War II, cohesion, or the bonds between soldiers, has traditionally been posited as the primary motivation for soldiers in combat.[142] Evaluating American soldiers in the early months of the 2003 Iraq war, Leonard Wong and a

---

[139] John Spencer, "From Army of One to Band of Tweeters," *The NewYork Times*, November 5, 2015, accessed November 15, 2015, http://www.nytimes.com/2015/11/05/opinion /from-army-of-one-to-band-of-tweeters.html?_r=0.

[140] Ibid.

[141] Spencer, "From Army of One."

[142] Leonard Wong, Thomas A. Kolditz, Raymond A. Millen, and Terrence M. Potter, *Why They Fight: Combat Motivation In The Iraq War* (Carlisle, PA: Strategic Studies Institute, 2003), accessed November 15, 2015, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB179.pdf.

team of researchers concluded that emotional bonds of trust between soldiers were what motivated them to fight within the context of that conflict. Notably, Wong's research highlighted the importance of communication outside of combat, "the hours of nothingness, the shared boredom, where bonds of trust, friendships and group identity are built." Today, increasing amounts of this nothing time is consumed online, emerged in virtual space. This observation does not discount the potential added benefits of improved communication between deployed soldiers and their families at home; however, recognition and study of the effects is increasingly important given future generations' lack of familiarity with being disconnected. For example, how will a lack or degradation of communication affect a soldier's mindset or performance in training or combat? The ability to be virtually and intimately connected to the everyday stressors of life back home adds a dynamic to conflict with implications well worth evaluating. Finally, the idea that a soldier may have a persona online that is perceived to be much different than his identity in physical space cannot be dismissed. To what extent do impressions in virtual space influence behavior in physical space and vice versa?

The Digital Immigrant and Digital Native Divide[143]

Generations born into this digitized world have fundamentally different understandings of what it means to live with and without cyberspace in comparison to those born into a pre-cyber enabled world.[144] While senior Army leaders and those among their generation have adapted to environments driven by cyber technical means, often relative to their personal curiosities, younger and future generations are only able to imagine life without instant and chronic information. The understanding that the communication of information and knowledge once emanated exclusively from physically known or trusted sources will

[143] For more on digital natives (those born into a world enhanced by cyber technology) versus digital immigrants (those who have adapted to a world enhanced by cyber technology,) see Mark Prensky, "Digital Natives, Digital Immigrants," *On the Horizon* 9, no.2, (2001): 1-6.

[144] P.W. Singer and Allan Friedman, *Cybersecurity and CyberWar: What Everyone Needs to Know* (New York, NY: Oxford University Press, 2014), 16.

likely be foreign to these digital natives.[145] This digital native understanding conflicts in many ways with the Army's hierarchical structure and may drastically challenge current models of indoctrination and concepts such as trust.

Currently, younger military officers and soldiers being taught and led are increasingly of the digital or millennial generation, and those teaching and leading them primarily are not. A study conducted by the Center for Research and Education on Aging and Technology Enhancement found that adults' attitudes toward technology are an important factor in predicting how comfortable they are in using it.[146] Adults who feel anxious or uncomfortable around technology, or who don't believe they have the aptitude to learn, are likely to avoid them.[147] The study suggests that independent of other factors, such as lack of exposure to technology or a previous bad experience, age matters. While the average teenager in the United States has grown up where "online" is as commonplace as hot water, technically-expert senior military leaders are scarce.[148] The difficulty of learning cyber language and techniques are not intuitive and again, given the speed of evolution, a difficult medium in which to stay current.[149]

As one consequence, some commanders view the environment of cyberspace as a leadership challenge to control. For example, regarding the social environment of cyberspace, some have limited the access soldiers have to their technology.[150] These responses are the result of understandings framed in old models ill-suited for current realities. Within the institutionally hierarchical Army organization, there

---

[145] Prensky, "Digital Natives, Digital Immigrants."

[146] Sara J. Czaja et al., "Factors Predicting the Use of Technology," *Psychology and Aging*, 21, no.2 (2006): 333-352.

[147] Ibid.

[148] Brickey, Cox, Nelson, and Conti, "The Case for Cyber."

[149] Timothy L. Thomas, "Hezballah, Israel and Cyber PSYOP," *IO Sphere* (Winter 2007): 24.

[150] Andrew B. Stipp, "Leading Soldiers with – Not Primarily Through – Communication Technology," *Military Review* (November-December 2015): 101-107.

exists an obvious cultural divide between more senior generations and younger generations, born into a world at the very least augmented by cyberspace but, as time goes by, into a world in which cyberspace and the "really real" merge seamlessly into a new everything.

Of equal and almost opposite concern for the Army is the increasing population of young people uncomfortable performing missions in analog settings. From socializing to banking to map reading, cyber technologies now form the base of understanding for those born in a cyber enabled world. Which military practitioner skills are best developed with cyber technology? Which historically "old fashioned" ways of executing Army operations should be preserved? For example, a recent study that sought to test how note-taking by hand or by computer affects learning determined the former was more beneficial as it developed critical thinking skills such as summarizing, paraphrasing, and concept mapping.[151] Yet another paradox of technology is that the more dependent society becomes on cyber technology, the more valuable critical thinking skills become.[152] Finally, how does the Army attract and retain young people interested and accustomed to living between both domains if the predominate language of the institution continues to minimize its potential, treating cyber technologies as mere capabilities?

Those who first recognize, understand, and implement processes that maximize the tools of all generations and prepare for the vulnerabilities associated with dependency will have the potential to gain a decisive advantage.[153] Conversely, a nation that is slow to adapt to new generational realities opens itself to catastrophic defeat. [154]

---

[151] James Doubek, "Attention Students: Put Your Laptops Away," National Public Radio, April 17, 2016, accessed April 17, 2016, http://www.npr.org/2016/04/17/474525392.

[152] Anna Davies, Devin Fidler and Marina Gorbis, "Future Work Skills 2020," *University of Phoenix Research Institute*, 2011, accessed March 10, 2016, http://www.cdn.theatlantic.com/static /front/docs/sponsored/phoenix/future_work_skills_2020.pdf.

[153] William S. Lind et al., "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, October 1989.

[154] Ibid.

Artificial Intelligence and the Army

The Army is on the cusp of a major transformation in the relationships it has with many of its tools. The development of autonomous capabilities is a critical component of the Pentagon's third offset strategy, which is "a research effort intended to endow the United States with strategic advantage over her adversaries."[155] Over the next decade, new and prolific "smart" machines will become integral to training, combat, soldier wellness, security, and nearly every aspect of military experience. This includes machine learning systems that search through volumes of data to find weak signals of social change for indicators to inform analytical assessments to cyber defensive operations flying drones and boats. The cyber technologies DARPA is pursing range from brain and prosthetic programs to the engineering of hunter – killer robots.[156] Deputy defense secretary Robert Work recently shared, "You cannot have a human operator operating at human speed fighting back at determined cyber tech. You are going to need to have a learning machine that does that."[157]

As cyber technical machines replace humans in some responsibilities, and augment them in others, it will require the institution confront important questions. What are human soldiers uniquely good at? What constitutes an appropriate soldier machine relationship? The Army will have to rethink how missions are executed and what processes shape their completion. In some cases, machines will become collaborators, augmenting soldier skills and abilities. Artificial intelligence will likely establish new expectations and standards of soldier performance. Army leaders will need to be increasingly aware of

[155] Patrick Tucker, "The Future of Cyber Analytics In the Department of Defense," *Defense One*, (April 2016), accessed April 15, 2016, www.defenseone.com/assets/future-cyber-analytics-department-defense/.

[156] Jacobson, 427.

[157] Tucker, "The Future of Cyber Analytics In the Department of Defense,"

what it means to partner with machines in a relationship that will build on mutual strengths and result in a new level of human-machine collaboration and codependence.

Conclusion

American astronomer Carl Sagan once stated, "It is suicidal to create a society dependent on science and technology in which hardly anybody knows anything about the science and technology."[158] While the statement is extreme, the message to the Army applies. The Army has become institutionally reliant on cyber technologies that most within the organization cannot intuitively break down. This is a relatively new experience for soldiers and comes with great and largely unknown implications. The situation is exacerbated by an institutional disconnect and reluctance to embrace the complexity and strategic potential of cyberspace, choosing instead to interpret the domain with tools and frameworks from the industrial era past.

James Rosenau argues that to think theoretically, one has to be able to go to the conceptual level, sacrifice detailed descriptions for broad observations, tolerate ambiguities, have concern about probabilities, and be distrustful of absolutes.[159] Conceptually, this work addresses the idea that cyber technologies create the potential to alter understandings of time, space, and identity both instantaneously and subversively. Studies and examples presented throughout this monograph suggest that military leaders charged with the design of military art are susceptible to falling victim to this powerful reality.

Notions of cyberspace as related to the development of military strategy achieve a level of observational and descriptive adequacy when they include (a) in-depth treatment of the variables of time and space as related to the contemporary operating environment and (b) proper weighting of the relationship between cyber technology and human behavior from both friendly and adversarial

---

[158] Jacobson, 424.

[159] James N. Rosenau, *The Scientific Study of Foreign Policy* (London: Frances Pinter, 1980), 19-31.

perspectives. Conceptualizations of cyberspace must meet these conditions because cyber technology compresses cognitive understandings of time and space with effects on all instruments of national power and culture and because cyber technology continues to alter how individuals and societies construct reality and express behavior.

Evidence in response to the first research question addressed how the Army accounts for the fundamental concepts of time and space, especially as related to cyberspace and the execution of operational art. The second question looked carefully at how the Army recognizes the role that cyberspace plays in identity formation and the social constructions of reality of both friendly and enemy actors. The work has demonstrated the existence and the extent of the gap between how the Army currently understands cyberspace and the author's proposed conditions of adequacy in conceptualizations of cyberspace. The gap identified is very understandable given the speed of innovation in cyber technology and the natural apprehension as to how to understand and exploit it, both of which exist amidst the glimmerings of increased uses of artificial intelligence and the highly evident indications that the role of human activity in war is changing.

The need for Army leaders and planners to function at a higher level of cyber conceptualization is apparent in every example the monograph has cited. With the given of an unknowable future, the military must figure out a way to deal with the paradox of maintaining perspective and control all the time, accepting that the cyber environment cannot be controlled. This paradox severely challenges a culture that has developed and thrived under linear rules and equation-based understandings of the world. The task is as daunting and immediate as any the Army has ever faced and only the uncertainty of the outcome is certain. The Army must protect its citizenry by fighting through the dualisms in which the rapid speed of change is pitted against bureaucratic inertia and dogged culture.

Despite the challenges ahead, optimism must remain the watchword of the Army's service to the United States. The US Army and a majority of those who serve within its ranks are motivated and resilient. Some of the required cultural changes will happen inevitably, as younger generations rise in rank. However, given the speed of cyber evolution and the grindingly slow process of institutional

change, the Army cannot afford to lose time. The future is now and the time has come to act. The author recommends as a first step of many, that the Army reconsider how it accounts for space and time throughout all of its doctrinal publications. This includes emphasis on the potential of cyber technologies throughout professional military education and training opportunities. As the operational environments today are dependent on various cyber technologies, the sooner the significance of cyberspace is broadened in doctrine and more directly addressed in training and education, all Army players on the battlefield will be better equipped.

The understanding of cyber technologies and their use in war should include strategic, temporal, geographic and human factors. The need for targeted research and theoretical and practical thinking on the effects of computer technology and warfare continues to grow. The title of this monograph was inspired, in part, by Daniel Kahneman's book *Thinking, Fast and Slow*. In it, Kahneman explains the two systems that drive the way humans think. One of the chapters of the book describes the significance of frames and reality in human decision making. Kahneman suggests that most people "passively accept decision problems as they are framed and therefore rarely have an opportunity to discover the extent to which our preferences are *frame-bound* rather than *reality-bound*."[160]

Cyber technologies are rapidly altering the military's operational environment, yet the Army largely still uses frames that do not factor this reality. From an organizational perspective, the issue is reminiscent in some ways to the Army in the interwar period.[161] The uncertain role of military aviation fueled the debate between those who saw technology as way to revolutionize warfare and "those who

[160] Daniel Kahneman, *Thinking Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 367.

[161] Peter W. Singer, "Lessons from Defense Strategy in the Interwar Years," *Brookings*, April 2013, accessed May 4, 2016,http://www.brookings.edu/research/articles/2013/08/strategic-defense-reform-singer.

clung to the past and saw machines merely as a means to improve existing concepts."[162] In considering cyberspace as primarily limited to the deployment of cyber capabilities, its strategic potential is easily overlooked. In war, the act of framing—the act of describing the operational environment, and thus determining decisions to be made—is a moral task. It is often *the* moral task. Cyber technologies are going to continue to alter perceptions of space and time and shape human behavior around the world whether or not the Army takes the implications of these facts seriously and in depth. The Army needs to find the courage to reconstruct itself in ways that will violate its historical understanding of its role and structure, and therefore will be very costly institutionally and, for some, personally. In order to be best prepared for the wars of today and wars of the future, it is time for the Army to accept a new reality proactively and reframe it with an institutional investment in an adequate conceptualization of cyber technology and its effects on war and warfare.

[162] David E. Johnson, "From Frontier Constabulary to Modern Army: The US Army between the World Wars," in *The Challenge of Change: Military Institutions and New Realities, 1918-1941*, ed. Harold R. Winton and David R. Mets (Lincoln: University of Nebraska Press, 2000), 173.

Bibliography

Army Doctrine Publication 3-0. *Unified Land Operations*. Washington, DC: Government Printing Office, 2012.

Army Doctrine Publication 5-0. *The Operations Process*. Washington, DC: Government Printing Office, 2012.

Army Doctrine Publication 1-01. *Doctrine Primer*. Washington, DC: Government Printing Office, 2014.

Army Doctrine Reference Publication 3-0. *Unified Land Operations*. Washington, DC: Government Printing Office, 2012.

Army Doctrine Reference Publication 3-90. *Offense and Defense*. Washington, DC: Government Printing Office, 2012.

Army Field Manual 3-38. *Cyber Electromagnetic Activities*. Washington, DC: Government Printing Office, 2014.

Allhoff, Fritz, and Patrick Lin, eds. *Nanotechnology and Society*. New York: Springer-Verlag, 2008.

Bender, Jason. "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations." *Small Wars Journal* (November 2013). Accessed January 10, 2016. http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner.

Berger, Peter L., and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge.* New York: Doubleday, 1967.

Blascovich, Jim, and Jeremy Bailenson. *Infinite Reality: Avatars, Eternal Life, New Worlds and the Dawn of the Virtual Revolution.* New York: HarperCollins, 2011.

Brantly, Aaron F. "Strategic Cyber Maneuver." *Small Wars Journal* (October 2015). Accessed November 12, 2015. http://smallwarsjournal.com/jrnl/art/strategic-cyber-manuever.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Group, 2011.

Brickey, Jon, Jacob Cox, John Nelson, and Gregory Conti. "The Case for Cyber." *Small Wars Journal*. (September 2012). Accessed January 5, 2016. http://smallwarsjournal.com/jrnl/art/the-case-for-cyber.

Bryant, Rebecca. "What Kind of Space is Cyberspace?" *Minerva - An Internet Journal of Philosophy* 5 (2001). Accessed March 11, 2016. http://www.minerva.mic.ul.ie//vol5/cyberspace.html.

Brynjolfsson, Erik, and Andrew McAfee. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York: W.W. Norton & Company, 2014.

Bunker, Robert J., and Charles Sid Heal. *Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and War-a Terrorism Research Center Book*. Bloomington, IN: iUniverse, 2014.

Case, Amber. *Calm Technology: Designing for Billions of Devices and the Internet of Things*. Sebastopol, CA: O'Reilly Media, 2015.

Cohen, Jared, and Eric Schmidt, *The New Digital Age: Reshaping the Future of People, Nations and Business.* New York: Random House, 2013.

Chomsky, Noam. *Syntactic Structures.* The Hague: Mouton, 1957.

Cuthbertson, Anthony. "US Military Launches Cyberattacks against ISIS." *Newsweek Magazine*, March 2, 2016. Accessed March 2, 2016. http://www.newsweek.com/us-military-launches-cyber-attacks-isis-432441.

Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security*. Athens, GA: University of Georgia Press, 2011.

D'Erasmo, Stacey. "Living on Internet Time," *New Yorker*, October 30, 2014. Accessed March 16, 2016. http://www.newyorker.com/books/page-turner/lost-time.

Delacruz, Victor. "Mission Command In and Through Cyberspace: A Primer for Army Commanders." *The Cyber Defense Review* (December 2015). Accessed December 20, 2015. http://www.cyberdefensereview.org/2015/12/10/mission-command-primer/.

Derian, James Der. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network*. 2nd ed. New York: Routledge, 2009.

Diener, C. *Borderlines and Borderlands: Political Oddities at the Edge of the Nation State*. Edited by Alexander C. Diener and Joshua Hagen. Lanham, MD: Rowman & Littlefield Publishing Group, 2009.

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

Dutton, William H., ed. *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press, 2014.

Elkus, Adam. "A Critical Perspective on Operational Art and Design Theory." *Small Wars Journal*. (April 2012). Accessed April 11, 2016. http://smallwarsjournal.com/jrnl/art/a-critical-perspective-on-operational-art-and-design-theory.

Elon University. "1830s-1860s: The Telegraph." Accessed 30 March 2016. http://www.elon.edu/e-web/predictions/150/1830.xhtml.

Frost, Patricia, and Matthew Hutchison. "The Top 10 Questions for Commanders to Ask About Cyber Security." *Small Wars Journal* (December 2015). Accessed February 11, 2016.

http://smallwarsjournal.com/jrnl.art/top-10-questions-for-commanders-to-ask-about-cybersecurity.

Gardner, Howard, and Katie Davis. *The App Generation: How Today's Youth Navigate Identity, Intimacy and Imagination in a Digital World*. New Haven: Yale University Press, 2013.

Garza, Gilbert. "The Internet, Narrative, and Subjectivity." *Journal of Constructivist Psychology*. 15 (2002): 185-203.

Gates, Scott, and Sukyana Podder. "Social Media, Recruitment, Allegiance and the Islamic State." *Perspectives on Terrorism* 9, no. 4 (2015). Accessed April 3, 2016. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/446/html.

Gladwell, Malcom. *Blink: The Power of Thinking Without Thinking*. New York: Little Brown and Company, 2005.

Graham, Mark, and William H. Dutton, eds. *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives*. Oxford: Oxford University Press, 2014.

Gray, Colin S. *The Future of Strategy*. Cambridge: Polity Press, 2015.

Guha, Manabrata, and Sam Bateman. *Reimagining War in the 21st Century: From Clausewitz to Network-Centric Warfare*. New York: Taylor & Francis, 2010.

Goodman, Marc. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. New York: Doubleday, 2015.

Greenfield, Susan. *Mind Change: How Digital Technologies Are Leaving Their Mark on Our Brains.* New York: Random House, 2015.

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

Harper, Caleb. "This Computer Will Grow Your Food in the Future" [video]. *TED Talks*. Posted March 2016. Accessed April 15, 2016. http://www.ted.com/talks/caleb_harper_this_computer _will_grow_your_food_in_the_future.

Hatch, Mary Jo, and Ann L. Cunliffe. *Organization Theory: Modern, Symbolic, and Postmodern Perspectives*. 2nd ed. New York: Oxford University Press, 2012.

Hayden, Michael V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press, 2016.

Institution of Engineering and Technology. "The first transatlantic telegraph cable 1858." Accessed March 12, 2016. http://www.theiet.org/resources/library/archives /featured/trans-cable1858.cfm.

Issacson, Walter. "The Future of the Human Spirit in a World of Machines." [video]. Posted May 14, 2015. Accessed October 11, 2015. http://www.smithsonianmag.com/videos/category/future-is-

here/future-is-here-festival-2015-walter-isaacson/#ooid=BwczB5dTrQqajwipRxK0OB xxcJxW0v7Z.

Jacobsen, Annie. *The Pentagon's Brain: An Uncensored History of DARPA, America's Top-Secret Military Research Agency*. New York: Little, Brown & Company, 2015.

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

Johnson, David E. "From Frontier Constabulary to Modern Army: The US Army between the World Wars." In *The Challenge of Change: Military Institutions and New Realities*, edited by Harold R. Winton and David R. Mets, 162-204. Lincoln: University of Nebraska Press, 2011.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

Kern, Sean Charles Gaines. "Expanding Combat Power Through Military Cyber Power Theory." *Joint Force Quarterly*, no.79 (2015): 88-94.

Kissinger, Henry. *World Order*. New York: Penguin Books, 2014.

Kruause, Michael D., and R. Cody Phillips, eds. *Historical Perspectives of the Operational Art*. Washington, DC: Center of Military History, 2007.

Kollmeyer, Barbara. "Want World Peace? Share much more on Facebook, Mark Zuckerberg says." *Market Watch*, February 26, 2016. Accessed March 16, 2016. http://www.marketwatch.com/story /facebooks-mark-zuckerberg-touts-more-sharing-as-a-route-to-world-peace-2016-02-26.

Leonhard, Robert. *Fighting by Minutes: Time and the Art of War*. Westport, CT: Greenwood Publishing Group, 1994.

Libicki, Martin. "Cyberspace is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2. (Fall 2012): 325-340.

Lind, William S. et al. "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, (October 1989): 22-26.

Lyngas, Sean. "Former NSA chief: Data manipulation an 'emerging art of war.'" *The Business of Federal Technology*, October 22, 2015. Accessed March 16, 2016. https://fcw.com/articles/2015/10/22 /alexander-data-manipulation.aspx.

McChrystal, Stanley A. *Team of Teams: New Rules of Engagement for a Complex World*. New York: Penguin Books, 2015.

McKinnon, Rebecca. "Ruling Facebookistan: The world's largest social networking site has a population nearly as large as China or India's. And the natives are getting restless." *Foreign Policy Magazine*, June 14, 2012. Accessed March 25, 2016. http://foreignpolicy.com/2012/06/14/ ruling-facebookistan/.

Melhem, Hisham. “Keeping Up with the Caliphate: An Islamic State for the Internet Age.” *Foreign Affairs* 94, no. 6 (2015): 148-153.

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

NATO Cooperative Defence Center of Excellence. “Cyber Definitions.” Accessed March 10, 2016. https://ccdcoe.org/cyber-definitions.html.

Paret, Peter. *Cognitive Challenge of War.* Princeton: Princeton University Press, 2009.

Poulsen, Kevin. *Kingpin: How One Hacker Took over the Billion-Dollar Cybercrime Underground*. New York: Random House, 2011.

Reynolds, Paul. “The Man Who Predicted the Great War.” *History Today* 20, no. 2 (2013). Accessed March 24, 2016. http://www.historytoday.com/paul-reynolds/man-who-predicted-great-war.

Rheingold, Howard. *Net Smart: How to Thrive Online*. Boston: MIT Press, 2014.

Rosenzweig, Paul. “Cyberwar is Here to Stay.” February 24, 2016. Accessed March 6, 2016. http://www.governing.com/templates/gov_print_article?id=370008341.

Rochlin, Gene. *Trapped in the Net: The Unanticipated Consequences of Computerization*. Princeton, NJ: Princeton University Press, 1997.

Ryan, Johnny. *A History of the Internet and the Digital Future*. London: University of Chicago Press, 2013.

Sandburg, Carl. *Chicago Poems*. New York, NY: Henry Holt and Company, 1916.

Scharre, Paul. “Uncertain Ground: Emerging Challenges in Land Warfare.” *Center for a New American Security* (December 2015): 6-7. Accessed January 3, 2016. https://www.cnas.org/emerging-challenges-in-land-warfare#.VyEFVhMrLGI.

Schiener, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control the World.* New York: W.W. Norton & Company, 2015.

Schnieder, James. “The Loose Marble – and Origins of Operational Art.” *Parameters* 19 (1989): 85-99.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. NewYork: PublicAffairs, 2016.

Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations*. New York: Penguin Group, 2009.

——— . *Cognitive Surplus: How Technology Makes Consumers into Collaborators*. New York: Penguin Group, 2010.

Sighholm, Johan. “Non-State Actors in Cyberspace Operations.” *Journal of Military Studies* 4, no.1 (2013): 32. Accessed October 15, 2015. http://ojs.tsv.fi/index.php/jms/article/view/7609/pdf_1.

Singer, Peter W, and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

——— . Testimony to Senate Armed Services Committee. Hearing on The Future of War. November 3, 2015. Accessed November 23, 2015. http://www.armed-services.senate.gov/imo/media/doc/Singer_11-03-15.pdf.

Steiner-Adair, Catherine, and Teresa H. Barker. *The Big Disconnect: Protecting Childhood and Family Relationships in the Digital Age*. New York: HarperCollins Publishers, 2013.

Stevens, Tim, and Peter R. Neumann. *Countering Online Radicalisation: A Strategy for Action*. London: International Centre for the Study of Radicalization and Political Violence, March 2009. Accessed April 11, 2016. https://cst.org.uk/docs/countering_online_radicalisation1.pdf.

Stipp, Andrew B. “Leading Soldiers with – Not Primarily Through – Communication Technology.” *Military Review* (November-December 2015): 101-107.

Spencer, John. “From Army of One to Band of Tweeters.” *New York Times*, November 5, 2015. Accessed November 15, 2015. http://www.nytimes.com/2015/11/05/opinion /from-army-of-one-to-band-of-tweeters.html?_r=0.

Taylor, Jonathan. “The Emerging Geographies of Virtual Worlds.” *Geographical Review*, 87, no. 2 (1997): 172-192.

Thomas, Timothy. “Creating Cyber Strategists: Escaping the ‘DIME’ Mnemonic*” Defence Studies* 14, no. 4 (2014): 370. Accessed January 5, 2016. http://dx.doi.org/10.1080 /14702436.2014.952522.

———. “Hezballah, Israel, and Cyber PSYOP.” *IO Sphere* (Winter 2007): 30-35. Accessed March 11, 2016. http://www.fmso.leavenworth.army.mil/documents/new-psyop.pdf.

Tikk-Ringas, Eneken, Mika Kerttunen, and Christopher Mika.“Cyber Security as Field of Military Education and Study.*” Joint Force Quarterly* 75 (4th QTR 2014): 57.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War.* New York: Warner Books, 1995.

Torrike-Barton, Dex. “How the internet is uniting the world.” *A Medium Corporation*, October 14, 2015. Accessed. October 14, 2015. https://medium.com/@dextbarton/how-the-internet-is-uniting-the-world-36408b457692#.7uzz7i54n.

Turabian, Kate L, Wayne C Booth, Gregory G. Colomb, Joseph M Williams, and University of University of Chicago Press Staff. *A Manual for Writers of Research Papers, Theses, and Dissertations, Eighth Edition: Chicago Style for Students and Researchers*. 8th ed. Chicago: University of Chicago Press, 2013.

Turkle, Sherry. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books, 2013.

Turner, Frank. “The Army in Cyberspace.” *National Security Watch*, 14-1. Institute of Land Warfare: 2014. Accessed March 16, 2016. http://www.ausa.org/publications/ilw/DigitalPublications /Documents/nsw14-1/files/1.html.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. Oxford: Oxford University Press, 1963.

US Department of Defense. *2017 Budget Fact Sheet*. Washington, DC: Department of Defense, 2016.

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

———. *The DoD Cyber Strategy*. Washington, DC: Department of Defense, 2015.

US President. NSDD 145. “National Policy on Telecommunications and Automated Information Systems Security, 1984.” National Archives Catalog. Accessed January 15, 2016. https://research.archives.gov/id/6879742.

Valeriano, Brandon, and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press, 2015.

Van Creveld, Martin. *Technology and War: From 2000 B. C. to the Present*. New York: Free Press, 1989.

VanDriel, Martha S. H. *Bridging the Planning Gap: Incorporating Cyberspace into Operational Planning* Carlisle, PA: Strategic Studies Institute, 2015. Accessed December 10, 2015. http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Bridging-the-planning-gap/2015/05/04

Virilio, Paul, Sylvère Lotringer, and Mark Polizzotti. *Pure War (Semiotext(e) / Foreign Agents)*. Cambridge, MA: Semiotexte, 2008.

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

Warf, Barney. *Time-Space Compression: Historical Geographies*. London: Routledge, 2008.

Watkinson, William. “ISIS threatens Facebook founder Mark Zuckerberg and Twitter CEO Jack Dorsey in chilling video.” *International Business Times*, February 25,2016. Accessed March 2, 2016. http://www.ibtimes.co.uk/isis-threatens-facebook-founder-mark-zuckerberg-twitter-ceo-jack-dorsey-chilling-video-1545849.

Wong, Leonard, Thomas A. Kolditz, Raymond A. Millen, and Terrence M. Potter. *Why They Fight: Combat Motivation in the Iraq War.* Carlisle, PA: Strategic Studies Institute, 2003. Accessed November 15, 2015. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB179.pdf.

Zimmer, Daniel T. *Programmatic Integration of Cyber into The the Institutional Domain of Leader Development*. Master of Military Art and Science Thesis. Command and General Staff College. 2015.