2018-12

BITS AND BULLETS: CYBER WARFARE IN MILITARY OPERATIONS

Deterding, Stephen L.; Safko, Blake

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BITS AND BULLETS:
CYBER WARFARE IN MILITARY OPERATIONS

by

Stephen L. Deterding and Blake Safko

December 2018

Thesis Advisor: John J. Arquilla
Second Reader: Ryan Maness

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE BITS AND BULLETS: CYBER WARFARE IN MILITARY OPERATIONS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Stephen L. Deterding and Blake Safko	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Experts have been predicting the onset of cyber warfare for decades. Yet, despite the relative ease and anonymity with which cyber-attacks can be conducted on military targets, the preponderance of historical cyber-related actions has been largely confined to the realms of espionage and crime. So far, close integration of cyberspace operations with terrestrial military operations is a rare, if slightly growing, occurrence in warfare.

While discussions about cyber warfare have raged in academia and government in recent years, they have primarily focused on the impacts and implications that cyberspace operations have at the strategic level of war. Comparatively little research has been done to analyze how cyberspace operations will impact the battlefield.

We propose a framework for military planners to envision ways that cyberspace operations can be used to affect the battlefield and integrate with terrestrial combat operations. We then apply that framework to analyze a thought experiment involving a hypothetical conflict on the Korean peninsula in an attempt to catch a glimpse of what cyberspace operations may mean for the future of land warfare.

14. SUBJECT TERMS cyber, Internet, cyber-war, MDB, CYBERCOM	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

BITS AND BULLETS: CYBER WARFARE IN MILITARY OPERATIONS

Stephen L. Deterding
Major, United States Army
BS, University of Central Missouri, 2007

Blake Safko
Major, United States Army
BA, The Citadel, 2007

Submitted in partial fulfillment of the
requirements for the degrees of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)**

and

MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

**NAVAL POSTGRADUATE SCHOOL
December 2018**

Approved by: John J. Arquilla
Advisor

Ryan Maness
Second Reader

John J. Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Experts have been predicting the onset of cyber warfare for decades. Yet, despite the relative ease and anonymity with which cyber-attacks can be conducted on military targets, the preponderance of historical cyber-related actions has been largely confined to the realms of espionage and crime. So far, close integration of cyberspace operations with terrestrial military operations is a rare, if slightly growing, occurrence in warfare.

While discussions about cyber warfare have raged in academia and government in recent years, they have primarily focused on the impacts and implications that cyberspace operations have at the strategic level of war. Comparatively little research has been done to analyze how cyberspace operations will impact the battlefield.

We propose a framework for military planners to envision ways that cyberspace operations can be used to affect the battlefield and integrate with terrestrial combat operations. We then apply that framework to analyze a thought experiment involving a hypothetical conflict on the Korean peninsula in an attempt to catch a glimpse of what cyberspace operations may mean for the future of land warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. THE GROWING IMPORTANCE OF CYBERSPACE ON THE MODERN BATTLEFIELD 1
A. INTRODUCTION 1
B. RESEARCH QUESTION 4
C. METHODOLOGY 5

II. INVESTIGATING CYBER AND ITS EFFECTS ON THE BATTLEFIELD 7
A. WHAT IS CYBER? 7
B. WHAT ARE THE BATTLEFIELD EFFECTS OF "CYBER"? 10
C. BUILDING A CONCEPTUAL FRAMEWORK 13
D. CONCLUSIONS FROM THE LITERATURE REVIEW 15

III. THOUGHT EXPERIMENT—PART I 17
A. INTRODUCTION 17
B. WHAT IS THE DODIN? 17
1. How Dependent Are U.S. Land Forces on the DODIN? 18
2. How Vulnerable Is the DODIN to Attack? 19
C. HOW DO BATTLEFIELD CYBERSPACE OPERATIONS IMPACT LAND FORCES? A KOREAN SCENARIO PART 1 23
D. CONCLUSION 29

IV. THOUGHT EXPERIMENT—PART II 33
A. INTRODUCTION 33
B. HOW DO BATTLEFIELD CYBERSPACE OPERATIONS IMPACT LAND FORCES? A KOREAN SCENARIO PART 2 33
C. CONCLUSION 45

V. ANALYSIS AND CONCLUSION 49
A. INTRODUCTION 49
B. SUMMARY OF FINDINGS 49
C. IMPLICATIONS 53
D. A WAY AHEAD: ORGANIZATIONAL PARALLELS TO HUMAN INTELLIGENCE OPERATIONS 57
E. MERGING BITS WITH BULLETS 58

LIST OF REFERENCES 61

INITIAL DISTRIBUTION LIST 71

LIST OF FIGURES

Figure 1. Framework 14

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APT	Advanced Persistent Threat
CCTV	Closed-Circuit Television
CIA	Central Intelligence Agency
CJSOTF	Combined Joint Special Operations Task Force
USCYBERCOM	United States Cyber Command
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DNS	Domain Name System
DODIN	Department of Defense Information Network
GAO	Government Accountability Office
HUMINT	Human Intelligence
ISP	Internet Service Providers
ISR	Intelligence, Surveillance, and Reconnaissance
JFHQ-DODIN	Joint Force Headquarters – Department of Defense Information Network
MACV-SOG	Military Assistance Command Vietnam-Studies and Observation Group
NIPRNET	Non-classified Internet Protocol Router Network
OODA	Observe, Orient, Decide, and Act
OPM	Office of Personnel Management
SECDEF	Secretary of Defense
USSOCOM	United States Special Operations Command
SOF	Special Operations Forces
TC-AIMS II	Transportation Coordinators Automated Information for Movement System II

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, we would like to thank our families for their patience and support through the many long nights of researching and writing. Now that this is done, we can go to Tahoe.

To Dr. Arquilla and Dr. Maness, our guides and mentors as we explored a world completely new to us, thank you for your patience and wisdom. Without you, we would surely still be writing Chapter I.

For all the hackers, specifically Dave, Devnull, Jon, and Bob, who took the time to make sure we were staying out of fantasy land and made us even more paranoid than when we started, you guys are awesome!

Finally, we would like to thank all those other patient listeners, selfless helpers, and consummate professionals who assisted us throughout this process here, at the Naval Postgraduate School, and from USCYBERCOM, the Cyber Center of Excellence, the National Training Center, The U.S. Army Capabilities Integration Center, and U.S. Army G2 Mad Scientist. Specifically, thank you to COL Rice, COL(Ret.) Jones, LTC Bair, MAJ Dvorak, Maj Wolfe, CPT Rich, Mr. Brubeck, Dr. Warner, Mr. Kerekanich, Allison, and many others whom we are surely forgetting. We appreciate all the help.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE GROWING IMPORTANCE OF CYBERSPACE ON THE MODERN BATTLEFIELD

A. INTRODUCTION

Experts have been predicting the onset of cyber warfare for decades. So far, digital espionage and crime have made up the preponderance of historical cyber-related actions, despite the purported ease and anonymity of executing cyber-attacks against military targets. Yet, close integration of cyberspace operations with terrestrial military operations is a rare, if slightly growing, occurrence in warfare.

In 2008, Russia invaded the small neighboring country of Georgia. Russian-coordinated cyber-attacks, in support of a conventional ground force invasion, degraded the government of Georgia's ability to communicate through the Internet.[1] From 2013 to 2015, Russia also used cyber warfare in support of its annexation of Crimea and the continued destabilization of Eastern Ukraine.[2] In 2016, the United States established Joint Task Force Areas to conduct cyberspace operations against the Islamic State in support of Operation Inherent Resolve.[3] It seems the use of cyber in warfare is growing.

In 1992, Arquilla and Ronfeldt were among the first to envision the changes that the Information Revolution would bring to warfare. They coined the term "cyberwar" and theorized about the potential effects of computers and networks on future virtual and physical battlespaces.[4] Most importantly, they viewed cyberwar not simply as military operations in cyberspace but as an operational concept centered on control or governance

---

[1] Max Gordon, "Lessons from the Front: A Case Study of Russian Cyber Warfare" (research report, Air Command and Staff College, December 2015), 11–12.

[2] Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO CCD COE Publications, 2015), 90–91.

[3] Ellen Nakashima and Missy Ryan, "U.S. Military Has Launched a New Digital War against the Islamic State," *Washington Post*, July 15, 2016, https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?noredirect=on&utm_term=.195fdff0287a.

[4] John Arquilla and David Ronfeldt, *Cyberwar Is Coming!* RP-223 (Santa Monica, CA: RAND, 1992): 33. Later published in *Comparative Strategy* (April-June) 1993, Vol. 14

of information: translating information dominance into battlefield dominance.[5] Since then, however, academic thought has focused more on the application of cyberspace operations as a tool of national power or as a form of strategic attack, principally on infrastructure.

Evidence of this strategic focus is readily apparent. In 1996, Molander, Riddile, Wilson, and a team of experts conducted a study on strategic information warfare. The study used a nuclear proliferation exercise known as "The Day After," which was built on a scenario of major regional conflict in the Persian Gulf, to explore cyber threats. The team defined "strategic information warfare" as damaging national information infrastructure through cyberspace and scoped their study accordingly.[6] They acknowledged that cyber vulnerabilities to military operations existed in the theater of conflict, yet they did not examine it in their study. Their study concluded that the cyber threat to national information infrastructure was so grave that "key national military strategy assumptions are obsolescent and inadequate" when confronted with the harsh potential of cyberattacks.[7]

Similarly, Rattray's *Strategic Warfare in Cyberspace* both exemplified the fascination with the strategic potential of the cyber domain and codified its use in fulfilling such a role. Rattray's concept was essentially a new form of strategic bombing. He justified this by postulating that information infrastructures would likely be centers of gravity for advanced nations like the United States. His analysis identified the shortfalls of strategic bombing and the four requirements for successful "strategic information operations."[8] Despite his admissions about possible limitations to the effectiveness of strategic cyber warfare, Rattray's ideas appear to have taken hold widely among senior political and military leaders around the world. The use of cyberspace operations for strategic warfare

---

[5] Arquilla and Ronfeldt, 6, 15, 23.

[6] Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND, 1996), 1.

[7] Molander, Riddile, Wilson, xvii.

[8] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 27, 77, 99–101.

or political coercion is by far the norm, while the use of cyberspace operations to affect the battlefield remains the exception.[9]

Despite this decades-long focus on the strategic potential of cyberspace to end wars and cripple nations, Valeriano, Jensen, and Maness have questioned the effectiveness of strategic cyber operations. Their study conducts an empirical evaluation of the success or failure of strategic cyber actions to coerce. They compiled a data set of 192 known cyber incidents and found only 5.7% achieved any coercive success.[10] They acknowledge that the purpose of different aggressive acts in cyberspace varies and that "cyber degradation" is the only strategy in cyberspace likely to affect an adversary's behavior. The rate of coercive success increases to over 30% when examining only instances of cyber degradation.[11] Overall, their work identifies a trend similar to analyses of the efficacy of strategic bombing[12]; when used alone, strategic cyber actions have little coercive effect.[13] They conclude that strategic cyber actions have the greatest coercive effect when used in conjunction with other elements of national power.[14]

---

[9] A brief history of open-source cyber events supports this point. Work by Stuxnet, Shamoon, and events in Estonia in 2007, and many other cases are examples of cyber being used as a form of strategic attack. The few well-known or acknowledged cases of cyber being used in support of military operations was Georgia in 2008 and JTF areas in the fight against ISIS. Jason Healey, "Learn Cyber Conflict History or Doom Yourself to Repeat It," *Armed Forces Journal*, December 17, 2013; Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar," *WIRED*, accessed November 23, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; "Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces," Reuters, January 23, 2017, https://www.reuters.com/article/us-saudi-cyber/saudi-telecoms-authority-says-cyber-attacks-have-targeted-websites-idUSKBN1571ZR.; Nakashima and Ryan, "U.S. Military Has Launched a New Digital War against the Islamic State."

[10] Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *Cyber Strategy: The Changing Character of Cyber Power and Coercion.* (New York: Oxford University Press, forthcoming), 29.

[11] Valeriano, Jensen, and Maness, 29.

[12] Pape argues that strategic bombing is one of the "least effective ways to use airpower" because punishing populations only works in long wars of attrition decided by materiel superiority. Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War*, Cornell Studies in Security Affairs (Ithaca, NY: Cornell University Press, 1996). 316–317, 327. Clodfelter concludes that short of nuclear annihilation, air power has proved an unreliable means for achieving political goals. Mark Clodfelter, *The Limits of Air Power* (New York: The Free Press, 1989).

[13] Valeriano, Jensen, and Maness, *Cyber Strategy*, 385.

[14] Valeriano, Jensen, and Maness, 7–8.

The current U.S. organizational design maintains cyber capabilities primarily at the strategic level, reflecting the dominant view of cyber warfare as a strategic tool.[15] However, U.S. forces are ever more reliant upon digital technology and operate in an increasingly interconnected and networked environment. The essential role computers play in every aspect of modern militaries is undeniable. Computers have been a critical part of almost every major piece of military hardware since the late 1980s.[16] Perhaps most critically, nearly all planning, coordinating, resourcing, and information gathering is done on networked computers. That means all plans, units, processes, and major weapon systems in modern militaries are theoretically accessible through cyberspace. U.S. forces risk losing their technological advantages on future battlefields if the cyber debate continues to focus primarily on the strategic level of war.

B. RESEARCH QUESTION

What are the implications of cyber for battle? Recent conflicts have provided few answers to this question. As of this writing, the brief Russo-Georgian War of 2008 is the only clear example of the close integration of offensive cyberspace operations with maneuver warfare.[17] The conflict in Ukraine from 2014 to the present is potentially emerging as a second, but only time will tell if the techniques, tactics, and procedures employed warrant such a claim.[18] Additionally, the cloak of secrecy surrounding cyberspace operations increases the difficulty in analyzing their effects on the battlefield. Due to this near-void of historical case studies available for analysis, addressing the gap requires taking a heuristic approach.

---

[15] In the *DoD Cyber Strategy* for 2015, USCYBERCOM identifies its three missions as defending DoD networks, defending the nation, and supporting military operations and contingency plans. Despite the third mission sounding operationally focused, the document describes that mission as a presidential or SECDEF determination to use cyber operations as part of a military campaign. Ashton Carter, *Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, 2015), 5–6.

[16] David Bellin and Gary Chapman, *Computers in Battle: Will They Work?*, (Harcourt Brace and Co, 1987), 62.

[17] Armed Forces Communications and Electronics Association, "The Russo-Georgian War (2008): The Role of the Cyber Attacks in the Conflict," May 24, 2012, 5–10, https://www.afcea.org/site/defense/cyber-committee.

[18] Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar."

Our research seeks to answer multiple questions about the cyber domain, its effects on the modern battlefield, and what those effects imply for land warfare. Our goal is to examine the impacts of cyberspace operations on military combat operations through a thought experiment designed to explore the opportunities and vulnerabilities cyberspace presents. To do that, however, we must first answer a few questions through a review of the available literature. What is cyber? What are its effects? How dependent are modern militaries on the cyber domain?

The scope of this study is limited to examining the impacts of cyberspace operations on land forces at the tactical and operational levels of war. While cyberspace operations have been thoroughly examined at the strategic level of war, the battlefield impacts of cyberspace operations have received far less attention. Focusing on the impacts to land warfare only is necessary to bound our research and enable us to explore a smaller set of impacts and implications more thoroughly than if we examined warfare in all of the physical domains.

C. METHODOLOGY

We will conduct a two-part thought experiment to investigate cyberspace operations on the battlefield. The thought experiment is set within a hypothetical conflict on the Korean peninsula between the Democratic People's Republic of Korea (DPRK, or North Korea) and the allied forces of the Republic of Korea and the United States. Prior to launching into the scenario, we examine military computer networks through the example of the Department of Defense Information Network (DODIN), by asking the following questions: What is the DODIN? How dependent are U.S. land forces on the DODIN? How vulnerable is the DODIN to attack? Through the thought experiment, we attempt to evaluate the impact of cyberspace operations on the modern battlefield in order to draw out the implications they bring to warfare.

The first part of the thought experiment envisions undetected compromise of U.S. classified networks during a clandestine reconnaissance mission into North Korea. The second part considers both sides using cyberspace operations to support high-intensity conflict on the Korean peninsula. Within the scenario, each use of cyberspace operations

is examined both for its feasibility and for its impacts on the battlefield. We evaluate these actions through a combination of open-source research and logical analytic processes. While we do not presume to have settled the debate over the implications of cyberspace operations for land warfare, we hope to provide a useful framework for analysis and a contribution to the body of academic and military thought on what this new domain means for future battlefields.

a. Way Ahead

There remains a significant gap in considering the many implications of cyber for land warfare and what that means for commanders planning and executing military campaigns. By analyzing the vulnerabilities and opportunities presented by the cyber domain, in line with the cyberwar concept of information dominance, we aim to provide insights into how this new technology might change the conduct of warfare. Has the emergence of the cyber domain shifted the offense-defense balance? Does it challenge the validity of the principles of war? Are modern armies organized and composed to leverage this new domain on the battlefield?

We present this thesis in three sections. In the first section, we introduce the study, elaborate upon our research question and methodology, explore the literature regarding the effects of the cyber domain, and present our analytical framework. In the second section, we conduct a two-part thought experiment, pursuing the line of questioning mentioned previously and exploring the impacts of cyberspace operations on land warfare. In the third section, we analyze our findings and draw conclusions regarding what the cyber domain implies for land warfare, in an attempt to provide a framework for designing better operational concepts for a cyber-enabled battlefield.

II. INVESTIGATING CYBER AND ITS EFFECTS ON THE BATTLEFIELD

A. WHAT IS CYBER?

"Cyber" was originally just a prefix. Yet in today's military and international relations dialogue, "cyber" has become both a prefix and a noun. But what do military officers and politicians mean when they say "cyber"? Uses and definitions vary. Words like "Cyberwar," "cyber power," "cyber weapons," "cyber-attacks," and "cyberspace" permeate academic literature, but what does a phrase like "We need to invest more in cyber" mean? From a military perspective, "cyber" is routinely defined as "cyberspace" or the "cyber domain." The two terms are synonymous and refer to all computer networks including the Internet, networks' resident data, and the machines connected to them.[19] Analyzing cyber at the domain level, rather than focusing on cyber weapons or cyber-attacks, provides the most holistic view of its impacts on warfare. Simply looking at the tools used in cyberspace is akin to analyzing Army weapons to determine the implications of ground combat on warfare.

Libicki considers cyber to be a subset of information warfare. He separated information warfare into seven forms, four of which could all be considered manifestations of cyber warfare today.[20] The first, command and control warfare, was attacking the systems through which a military commands and controls its forces.[21] The second, hacker warfare, he defined as attacking civilian systems through the Internet.[22] The third, electronic warfare, he defined as an attempt to "degrade the physical basis for transferring information."[23] The fourth, cyber warfare, he considered at the time, to be in the realm of fantasy and included such things as virtual terrorism, semantic attacks, and simulation

---

[19] Joint Staff Director of Operations, "Joint Publication 3–12 (R) Cyberspace Operations" (Joint Staff, February 5, 2013), v.

[20] Martin Libicki, *What Is Information Warfare?* (National Defense University, 1995), 7.

[21] Libicki, 9.

[22] Libicki, 49–50.

[23] Libicki, 27.

warfare.[24] While very precise when analyzing the different ways to conduct information warfare, Libicki's definition of cyberwarfare has less to say about the presence of cyberspace on the battlefield and instead considers cyberspace to be *the* battlefield.

Kello analyzed cyber by focusing on weapons in cyberspace, primarily malicious code that affects the data or behavior of machines.[25] However, he did so at the strategic level, arguing that it has been incorrectly integrated into existing doctrines of international relations and war.[26] Kello also assessed that cyber was "an imperfect tool of interstate coercion" that had not yet transformed warfare or affected the balance of power between states.[27] Specifically, in the context of warfare he claimed that there has never been, and perhaps will never be, a true act of cyberwar, as cyber cannot replace military power but only augment its use.[28]

This last assertion, however, displays a fundamental and widespread misunderstanding of the role of cyber in military operations. Kello is analyzing the strategic level of war and cyber as an instrument of national power, in the vein of Joseph Nye who coined the term "cyber power,"[29] associating cyberwar with Libicki's definition as simulation warfare. When he claims that cyber has not transformed warfare, he is not speaking of how armies fight on the battlefield but instead how warfare is an instrument of statecraft. Yet, cyber might well be in the process of transforming the way armies deploy, array, and employ their forces in combat on the battlefield, thus transforming warfare.

Arquilla and Ronfeldt coined the term "cyberwar" and defined it as a battlefield concept focused on governing or controlling information.[30] In their study, *Cyberwar is*

---

[24] Libicki, 75.

[25] Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), 1.

[26] Kello, 3.

[27] Kello, 119–21.

[28] Kello, 121.

[29] Nye defines cyber power as, "resources that relate to the creation, control, and communication of electronic and computer-based information," which can be used to create effects both inside and outside of cyberspace. Joseph S. Nye Jr., *The Future of Power* (New York, NY: Public Affairs, 2011), 123.

[30] Arquilla and Ronfeldt, *Cyberwar Is Coming!*, 4.

Coming!, they theorized about the implications of the Information Revolution for warfare. One of their key observations was the notion that cyberwar was not just hackers fighting in cyberspace but included the idea that control of information would give military forces a decisive battlefield advantage.[31] In the 26 years since their study, the discussion about cyberspace and warfare has been conducted primarily in the strategic context, and thought about the impacts of cyberspace on warfare has been largely sidelined.

While U.S. doctrine recommends the integration of cyber operations into joint force operations, it notes significant challenges to doing so, such as the centralization of cyber operations planning, the need for the joint force to synchronize fires and operations, de-confliction between many actors, and legal considerations.[32] However, the U.S. Army is developing an operational concept called multi-domain battle that emphasizes the integration of all warfighting domains with less regard for time and space.[33] This concept claims new technologies and the trans-regional nature of current and future conflicts have expanded the battlespace, potentially unbounded by geography and with much-compressed timeframes. Multi-domain battle seeks to converge capabilities across all domains to create windows of opportunity to "defeat enemy systems and achieve friendly objectives outright."[34]

This new operational concept considers space, cyberspace, electronic warfare, and information critical components of enemy and friendly operations that potentially threaten all forces regardless of geographic disposition. Specifically, regarding cyber effects on the battlefield, multi-domain battle predicts that U.S. adversaries will use cyber from the deep fires area to target U.S. networks and space-based systems, disrupting operations and U.S. forces' ability to conduct decentralized mission command.[35] However, for the enemy to

---

[31] Arquilla and Ronfeldt, 6, 15, 23.

[32] Joint Staff Director of Operations, "Joint Publication 3–12 (R) Cyberspace Operations," vi.

[33] U.S. Army Training and Doctrine Command, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century" (Washington, DC: U.S. Army Training and Doctrine Command, December 2017), 6–7.

[34] U.S. Army Training and Doctrine Command, 4.

[35] U.S. Army Training and Doctrine Command, 18.

conduct these types of operations successfully requires significant preparation and mapping of U.S. systems and networks.[36]

While it appears that the U.S. Army recognizes the significant potential to either enhance or disrupt military operations that cyberspace has brought to the battlefield, tactical units currently lack the organic capabilities to leverage the effects of this new domain.

B. WHAT ARE THE BATTLEFIELD EFFECTS OF "CYBER"?

The Information Revolution of the late 20th century was ushered in by the rise of the digital computer. As computers increased in power and decreased in size, they were integrated into every piece of military hardware imaginable.[37] Computerized weapons and systems brought incredible technological capabilities to military forces including long-range precision fires, global communications, large sensor webs, and data processing and analytics.[38] With the invention of packet switching, computer systems were networked together and cyberspace, or the cyber domain, was born.[39] Thus, an important effect of cyberspace on the modern battlefield is that it connects high-technology weapons and information systems, enhancing their capabilities while also increasing their vulnerability to attacks through this new domain.

Rona was one of the first to recognize this increasing vulnerability of high-technology weapon systems in 1976. His characterization of the nature of advanced weapons, in that they consisted of physically separate but integrated subsystems with greatly increased external information flows, has risen in importance with the growth of

---

[36] U.S. Army Training and Doctrine Command, 26.

[37] As early as the mid-1980s, computers were considered the most important component in every major weapons system in development at the time. David Bellin and Gary Chapman, *Computers in Battle: Will They Work?* First Edition (Harcourt Brace and Co, 1987), 62.

[38] Bellin and Chapman, 66–68, 70, 81–90.

[39] The invention of packet switching is widely considered the foundational technology that led to the invention of the Internet. Barry M. Leiner et al., "Brief History of the Internet," *Internet Society* (blog), accessed June 19, 2018, https://www.internetsociety.org/Internet/history-Internet/brief-history-Internet/.

cyberspace.[40] He claimed that the performance of advanced weapons systems depended upon the integrity and availability of their external information flows, making them vulnerable to countermeasures targeted at those flows.[41] Rona specifically noted that denial, disruption, or manipulation of external information flows might become the primary method by which a belligerent seeks to protect its forces against advanced weapons systems such a precision munitions or cruise missiles.[42]

Arquilla and Ronfeldt's ideas about cyberwar align with Rona's insights about the growing importance of information flows. As they refined their ideas over the years, Arquilla maintained that a critical implication of cyberwar was the importance of achieving and maintaining the information edge.[43] In his opinion, having the information edge provided a decisive advantage on the battlefield because Information Revolution technologies empowered advanced militaries by providing enhanced situational awareness, precise overwhelming firepower, and unparalleled connectivity to the warfighter at the tactical level.[44] However, dependence on those same technologies makes advanced militaries vulnerable to disruption.[45] This disruption can be achieved through physical attacks on sensors or systems, jamming of signals, or through cyberspace. Thus, having the information edge means not just knowing more than one's enemy but also being able to employ high-technology systems while denying or disrupting those of the opponent.

Libicki argued that the networking of military weapons and information systems created a new center of gravity for advanced militaries, yet he focused on influencing the decision-making of the opponent rather than the integration of cyber and maneuver

---

[40] Thomas P. Rona, *Weapon Systems and Information War* (Washington, DC: Office of the Secretary of Defense, 1976), 11–13.

[41] Rona, vi, 1.

[42] Rona, 10.

[43] John Arquilla, "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers," *Communications of the ACM* 54, no. 10 (October 2011): 58, 60.

[44] John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA, 2000), 4–6.

[45] Arquilla, "From Blitzkrieg to Bitskrieg," 60.

warfare.[46] He viewed cyber weapons generally as inaccurate and not dependable, claiming integrating them with military operations would be problematic.[47] He asserts, "If one cannot predict the effects of information warfare on the adversary, one cannot begin to trade it off for or synchronize it with other forms of warfare."[48]

Berkowitz claimed that future wars would be fought on combined cyber and physical battlefields and that victory would first require winning the war over information.[49] Some of the critical aspects of this new face of warfare included the vulnerability of massed armies, network organizational structures, and "information armor" consisting of dispersion, covertness, and stealth.[50] He noted the four most important ideas that affect modern war are asymmetry, information war, cyberwar, and the observe, orient, decide, and act (OODA) loop.[51]

Gartzke points out that cyber-attacks will prove potent only when they are used in conjunction with or followed up by military force.[52] His overall argument is that strategic cyberwar is unlikely to be significant in world affairs because the Internet cannot replace physical force in a conflict.[53] Additionally, because the effects of a cyber-attack are temporary the value of cyber in battle is in creating short windows of surprise effects that can only be harnessed when used in conjunction with terrestrial military operations.[54] As a result, he suggests that cyberspace will not empower smaller and weaker groups but will

---

[46] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 1–12, 20.

[47] Libicki, 99.

[48] Libicki.

[49] Bruce Berkowitz, The New Face of War: How War Will Be Fought in the 21st Century (New York: The Free Press, 2003), 1.

[50] Berkowitz, 15–20.

[51] Berkowitz, 75.

[52] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 43.

[53] Gartzke, 42.

[54] Gartzke, 47–58.

instead increase the advantages of strong military powers that can exploit windows of opportunity with significant military force.[55]

Gartzke, like Kello, tends to equate the term "cyberwar" with the idea of a conflict between nations to occur in cyberspace without the need for armies in the field. Their conclusions are affirmations of the original cyberwar concept rather than refutations of it. Cyberwar calls for the integration of cyber capabilities with battlefield maneuver, not the replacement of one with the other.[56] All these experts mentioned in this section seem to agree that cyberspace operations will only be valuable in battle when integrated with military operations in the physical domains.

C. BUILDING A CONCEPTUAL FRAMEWORK

In an attempt to visualize the impacts of cyberspace on the battlefield, we designed a conceptual framework illustrating how it interacts with the other physical domains.

---

[55] Gartzke, 43.

[56] Arquilla and Ronfeldt state "cyberwar and netwar can be facilitated by, but do not necessarily depend on, 'the Net' (i.e., the Internet); nor do they occur only in 'cyberspace' or the 'infosphere.'" John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997), 7.

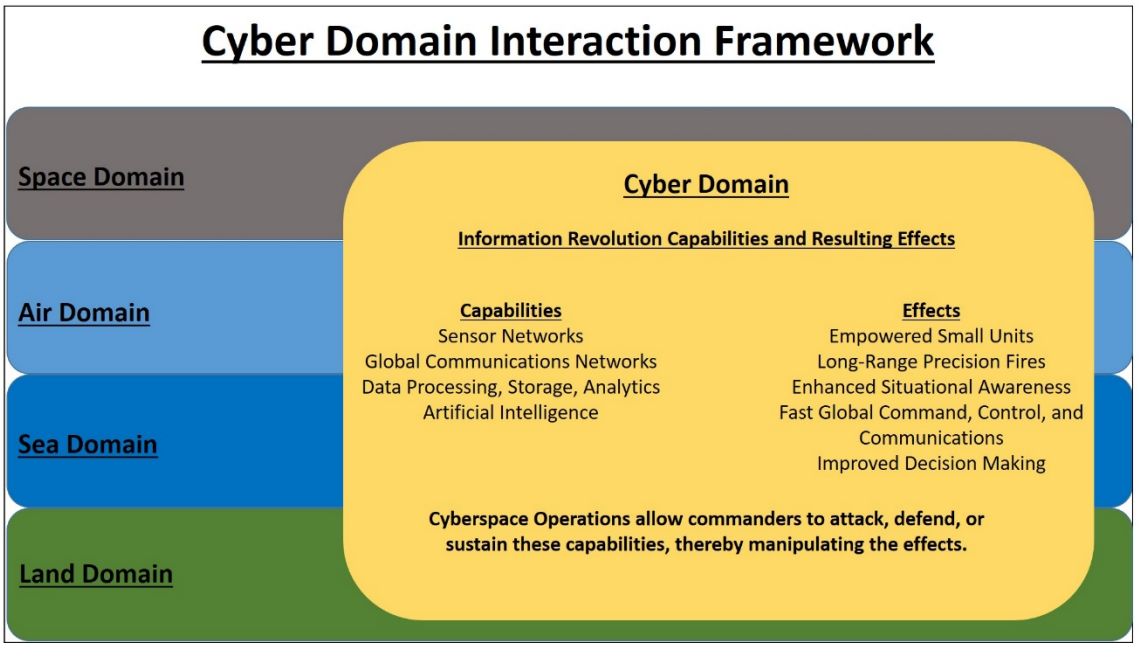

Figure 1. Cyber Domain Interaction Framework

The cyber domain is physically separated from the other domains. Sea touches land, both of which touch the air, and ascend high enough air becomes space. Land, sea, air, and space forces can all potentially attack each other directly with physical weapons. This is not entirely true of cyberspace. The only way the other domains physically "touch" cyberspace is through the infrastructure that creates and sustains it, and the machines that connect to it. Thus, while an air raid could bomb a physical server in an attempt to destroy a cyber weapon, if that weapon was stored in the cloud or backed up in a different physical location, then the air raid will have failed.

Conversely, however, a physical machine could be directly targeted and even destroyed by a cyberattack. For example, a drone could be hacked and forced to land in the wrong location, falling into the hands of the enemy.[57] This is not a hypothetical example, but one that has already occurred. In 2011, a U.S. drone was hacked and forced to land in Iran, resulting in the capture of an advanced U.S. system.

57 "How to Hack a Military Drone," Defense One, accessed June 5, 2018, https://www.defenseone.com/technology/2015/04/how-hack-military-drone/111391/.

In addition to illustrating the physical separation of the cyber domain from the traditional domains, the framework also highlights five major effects the cyber domain manifests on the battlefield. It creates these effects by connecting and facilitating computer-based technological capabilities such as networked sensor systems, global communication networks, and data processing and analytics. It also notes that cyberspace operations are a means by which commanders attack, defend, or facilitate the three technological capabilities, thereby tampering with their resulting effects. This seems like a simple conclusion, but it is an important deduction. U.S. Joint Publication 3-12R classifies three types of cyberspace operations: offensive, defensive, and DODIN.[58] DODIN operations, which include routine use of networks, are what manifest, facilitate, or sustain the effects previously noted. Defensive operations protect the DODIN and offensive operations attack the enemy's ability to manifest the same battlefield effects. If cyberspace enables long-range precision fires, then cyberspace can be the conduit to disrupt, degrade, deny, or destroy the enemy's capability to conduct them. If cyberspace enhances decision-making through expansive sensor webs, big data analytics, and artificial intelligence, then that decision-making can be slowed down, corrupted, deceived, or disrupted through offensive cyberspace operations.

D. CONCLUSIONS FROM THE LITERATURE REVIEW

Definitions of and ideas about what cyber *is* abound. In an attempt at precision, we use the following definitions and terms. In accordance with Joint Publication 3-12R, cyberspace and the cyber domain are synonymous and refer to all computer networks, the data on those networks, and embedded processors and controllers.[59] Cyberspace operations are military actions conducted in cyberspace.[60] As defined by Kello, Cyber weapons are malicious code that manipulates data and/or machines.[61] As conceived by Arquilla and Ronfeldt, cyberwar is an operational concept that views cyberspace operations integrated

---

58 Joint Staff Director of Operations, "Joint Publication 3–12 (R) Cyberspace Operations," II-2.

59 Joint Staff Director of Operations, v.

60 Joint Staff Director of Operations, v.

61 Lucas Kello, The Virtual Weapon and International Order, 1.

with physical military operations to achieve a decisive advantage in battle.[62] We avoid using the terms "cyber warfare" and "information warfare" as "cyber warfare" generally refers to cyberspace operations to achieve strategic objectives as opposed to cyberspace operations on the battlefield, and "information warfare" is a larger concept that focuses on disrupting the decision-making of the enemy. We try to minimize any additional use of the word "cyber" outside of these definitions as much as possible, but recognize that its use is sometimes necessary to specify an action occurring in cyberspace as opposed to the other domains.

Our review of the literature indicates the cyber domain manifests five major battlefield effects by connecting and facilitating technological capabilities. These capabilities broadly fall under the following categories: sensor networks, global communication networks, data processing, and artificial intelligence. The five major effects these capabilities manifest on the battlefield include empowered small units, long-range precision fires, enhanced situational awareness, fast global communications, and improved decision-making. Finally, cyberspace operations will be most effective on the modern battlefield when integrated with physical military operations.

To harness the effects of cyberspace in battle, warfighting doctrine requires reassessment. This reassessment should include the principles of war; traditional thought on objectives, decisive points, and centers of gravity; impacts to time, space, and force considerations; and the offense/defense balance. While a complete reassessment of operational doctrine in light of the effects of cyberspace is outside the scope of this thesis, we use the results of our thought experiment to identify which traditional concepts may be challenged by the rise of the cyber domain.

Critically, none of the effects noted in our framework result from the use of cyber weapons; they are simply reflections of the broader impacts the cyber domain has on the battlefield. In our opinion, a joint force will better employ cyberspace operations in battle if it views them in terms of how they can manipulate the battlefield effects of the cyber domain.

---

[62] Arquilla and Ronfeldt, *Cyberwar Is Coming!,* 4.

III. THOUGHT EXPERIMENT—PART I

A. INTRODUCTION

Extensive use of computers and networks characterizes modern militaries, especially the U.S. Armed Forces. The Information Revolution and the corresponding Revolution in Military Affairs that captured the U.S. military's attention in the 1980s and 1990s showed how computer networks could transform armed forces. As a result, cyberspace now connects many critical functions and capabilities of the U.S. military as well as other modern militaries with similar technologically advanced weaponry. This chapter seeks to evaluate the impacts of cyberspace operations on land warfare when integrated with terrestrial military forces. Understanding such potential impacts requires taking a closer look at how dependent modern militaries are on cyberspace. As a representative example, we analyze the largest military communications network in the world: the United States Department of Defense Information Network, or DODIN.

B. WHAT IS THE DODIN?

The DODIN is "all networks and information systems owned or leased by DOD."[63] It can be thought of as the U.S. military's territory in cyberspace, though portions of it also connect to the Internet. The DODIN's physical network consists of computers, servers, cables, and satellites; supporting voice, data, and video and messaging services around the globe.[64]

The DODIN is unique when compared to historical communication networks due to the breadth of military functions reliant on it. It is similar to early communication technologies, such as the telegraph, in that it enables swift communication across vast distances. Parallels even exist between telegraph and DODIN network protocols. The exchange between two computers using the eight-digit binary byte mirrors the eight-panel

---

63 Joint Chiefs of Staff, *Joint Communications System* JP 6–0 (Washington, DC: Joint Chiefs of Staff, 2015), viii, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf.

64 Joint Chiefs of Staff, II-13.

shutter telegraph from the mid-1800s.[65] While the telegraph rapidly spread across the world, it also had significant strategic impact on the conduct of the American Civil War.[66] However, the prohibitive transaction costs and inability to reach multiple end-users simultaneously prevented the level of dependence on the telegraph system that we see on the DODIN today.

Information flows across the DODIN via the electromagnetic spectrum to create, exchange, and store information across multiple domains—to numerous users—in near real-time.[67] The purpose of DODIN operations is to assure system and network availability, authenticity, information protection, and information delivery, all acting to protect and maintain freedom of action for the DOD across cyberspace.[68] Never before could information flow simultaneously in all directions between air, naval, and space-based platforms to soldiers operating on the frontiers of distant lands.[69]

1. How Dependent Are U.S. Land Forces on the DODIN?

The ability to share information across countless nodes in real time theoretically provides unmatched situational awareness and improves decision-making. However, the DODIN does not just facilitate communication. The Army describes the DODIN as a "critical warfighting platform" supporting all operations by enabling command and control of dispersed forces as well as by guiding precise fires, disseminating intelligence, and providing logistics support for those forces.[70] Additionally, Army computers, networks, and cloud services are the repository of vast stockpiles of data and are the default means by which to build and communicate briefings and plans. As our cyber domain interaction

---

65 Tom Standage, The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's Online Pioneers (New York: Bloomsbury, 1998), 206.

66 David Hochfelder, "The Telegraph," Essential Civil War Curriculum, Novembe14, 2018, https://www.essentialcivilwarcurriculum.com/the-telegraph.html.

67 Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, 1st ed. (Washington, DC: National Defense University Press, 2009), Chapter 2.

68 Joint Chiefs of Staff, *Joint Communications System,* II-2.

69 Kramer, Starr, and Wentz, *Cyberpower and National Security*, Chapter 2.

70 Headquarters, Department of the Army, *Cyberspace and Electronic Warfare Operations*, FM 3–12 (Washington, DC: Department of the Army, 2017), 1–1.

framework illustrates, while nearly all communications in the Army rely upon the DODIN in some way, the Army's high technology capabilities are also inextricably tied to it as well.

How does this dependency manifest on the battlefield? As demonstrated as early as Operation Desert Storm in 1991, a critical strength of the modern U.S. military has been its ability to synchronize parallel operations across the battlespace.[71] This high level of synchronization is a central tenet of the idea of Network-Centric Warfare. Network-Centric Warfare is an "information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[72] It calls for an architecture that consists of three grids: an information grid, a sensor grid, and a transaction grid.[73] The DODIN serves as the information grid in this concept, enabling numerous battlefield functions such as intelligence, surveillance and reconnaissance, long-range precision fires, synchronized battlefield maneuver, and systematic logistical support. As a result, the DODIN also represents a key vulnerability to exploit by enemies employing cyberwar concepts.

2. How Vulnerable Is the DODIN to Attack?

The DODIN's most significant vulnerabilities are due to the fact that it is an amalgamation of thousands of networks that were created separately and later bundled together in an attempt to improve security. As late as 2016, it was described as a "quasi-feudal patchwork of often incompatible local networks."[74] However, in just the past few

---

71 Arquilla and Ronfeldt, *In Athena's Camp,* 85.

72 David S. Alberts, John Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series (Washington, DC: National Defense University Press, 1999), 2.

73 Arthur K. Cebrowski and John Garstka, "Network-Centric Warfare: Its Origin and Future," *United States Naval Institute. Proceedings* 124, no 1(January 1998): 28–35, Proquest.

74 "Artificial Intelligence for Air Force: Cyber & Electronic Warfare," *Breaking Defense* (blog), accessed August 15, 2018, https://breakingdefense.com/2016/09/artificial-intelligence-for-the-air-force-cyber-electronic-warfare/.

years, U.S. Cyber Command (USCYBERCOM) and its subordinate command Joint Forces Headquarters-DODIN have attempted to address these issues through multiple initiatives such as the Joint Information Environment, Operation Gladiator Shield, and the creation of joint regional security stacks.[75] Despite these efforts, the DODIN is still subject to daily attacks that take on many forms and range in severity and duration. Attackers range from lone-wolf hackers to organized criminals and adversary nations. Some examples that highlight these vulnerabilities include the Agent.btz virus, the Office of Personnel Management (OPM) breach, Moonlight Maze, and satellite hacking.

In 2008, the U.S. military banned thumb drives in reaction to the Agent.btz virus.[76] It infected U.S. CENTCOM computers as well as hundreds of thousands of others around the world. The worm was designed to propagate widely and then send information about the infected systems to the controllers.[77] Agent.btz demonstrated the feasibility and relative ease with which an adversary using a cyberspace operation could gain access to highly sensitive areas of the DODIN, potentially compromising operational information. If the United States had been at war with Russia rather than at war in Iraq and Afghanistan, the battlefield consequences of such a breach could have been grave.

The 2015 OPM breaches demonstrated the sheer volume of information that can be acquired via a compromise of U.S. government networks and the incredibly sensitive

---

[75] The Joint Information Environment was a DoD effort to centralize and standardize information technology infrastructure across the department. Joint Regional Security Stacks centralize network security infrastructure into regions rather than at each military base. Operation Gladiator Shield is JFHQ-DODIN's initiative to map the cyber terrain of the DODIN and organize it into 42 operational areas. Defense Information Systems Agency, *Enabling the Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow* (Washington, DC: Defense Information Systems Agency, May 2014), 1–2, https://www.disa.mil/-/media/Files/DISA/About/JIE101_000.pdf; Defense Information Systems Agency, "JRSS Fact Sheet" (Defense Information Systems Agency, April 2017), https://disa.mil/-/media/Files/DISA/Fact-Sheets/JRSS-Fact-Sheet-April-2017.ashx?la=en&hash=68A0F70E92526693C2B824E49068DD52D78091D8; "Operation Gladiator Shield Targeting DoD's Cyber Terrain," FederalNewsRadio, February 20, 2018, https://federalnewsradio.com/cybersecurity/2018/02/operation-gladiator-shield-targeting-dods-cyber-terrain/.

[76] Elinor Mills, "USB Devices Spreading Viruses," CNET, November 20, 2008, http://news.cnet.com/8301-1009_3-10104496-83.html.

[77] Jim Finkle, "Agent.BTZ Spyware Hit Europe Hard after U.S. Military Attack: Security Firm," Reuters, March 12, 2014, https://www.reuters.com/article/us-russia-cyberespionage-idUSBREA2B25R20140312.

nature of the information available on networks like the DODIN. Together, two breaches compromised the personal data—to include social security numbers and fingerprints—of over 25 million government employees and their families.[78] Imagine if this information were released online. Identity theft would be the most common, but probably least significant, result for the victims of this attack. What might a global terrorist group do with such information? They could post kill lists on social media, not just of Soldiers but also of their wives, husbands, children, parents, or siblings. Perhaps they would even filter and sort their kill lists by U.S. units deployed to combat, complete with addresses and phone numbers of family members on the list. The battlefield effects of such an act would be hard to imagine. Would the posting of such a list affect the ability of deployed Soldiers to focus on their mission? Would cases of desertion increase? This massive theft of sensitive personnel information for such a large percentage of the federal workforce highlights the vulnerability of information at rest and serves as an indicator of the potential impacts of a breach of the of the DODIN.

One of the earliest cyber-espionage campaigns conducted against the United States occurred between 1996 and 1999.[79] Moonlight Maze refers to the investigations of a series of cyberattacks, initially detected in June 1998, purportedly aimed at stealing sensitive military technology information.[80] While Moonlight Maze was a series of intrusions, when viewed together with the OPM breach, these incidents highlight the significant length of time during which an adversary can gather information within a system before being detected.

Satellites are vital components of the DODIN that enable it to provide global communications support. Considering the DODIN is a critical capability for the DOD, the satellite infrastructure that gives it global reach might also be its critical vulnerability.

---

[78] "OPM Cybersecurity Incidents," Office of Personnel Management, June 12, 2018, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

[79] Kaspersky, "Moonlight Maze: Lessons from History," *Kaspersky Labs Daily* (blog), April 3, 2017, https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/.

[80] Chris Doman, "The First Cyber Espionage Attacks: How Operation Moonlight Maze Made History," Medium, July 7, 2016, https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7.

Satellites face many threats to deny, degrade, or disrupt the services they provide, and may even be targeted for destruction.[81] Destructive attacks, especially by physical or cyberspace operations, however, are less likely than disruptive attacks simply because of the response they would provoke. The current policy of the United States declares dominance in space a necessity and that any attacks on our critical space architecture will provoke a severe response.[82] Nevertheless, strategic competitors and potential adversaries are developing anti-satellite weapons, and satellite hacking, jamming, and spoofing are rising in frequency and prominence.[83]

While destructive attacks on U.S. space systems would likely result in immediate retaliatory strikes against the aggressor's satellites, temporary jamming or disruption might not be answered with a destructive, or even immediate, response unless such attacks cause significant battlefield effects or loss of life.[84] A unit in combat dependent on satellite

---

[81] "National Security Space Strategy" U.S. Department of Defense, January 2011, 3, https://www.defense.gov/News/Special-Reports/National-Security-Space-Strategy/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_/.

[82] "Remarks by Vice President Pence on the Future of the U.S. Military in Space," White House, accessed August 31, 2018, https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-future-u-s-military-space/; *National Security Strategy of the United States of America* (Washington, DC: White House, 2017), 31, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[83] White House, *National Security Strategy,* 31; Paul Rincon, "Russia Tests 'Satellite Catcher'" BBC News, November 20, 2014, https://www.bbc.com/news/science-environment-30097643; Murray Craig, "China Missile Launch May Have Tested Part of a New Anti- Satellite Capability" (staff research report, Washington, DC: U.S.-China Economic and Security Review Commission, May 22, 2013), https://www.uscc.gov/sites/default/files/Research/China%20Missile%20Launch%20May%20Have%20Tested%20Part%20of%20a%20New%20Anti-Satellite%20Capability_05.22.13.pdf.; J. M. Porup, "It's Surprisingly Simple to Hack a Satellite," *Motherboard* (blog), August 21, 2015, https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

[84] We believe this is a fair assumption considering the lack of any response to a series of satellite tampering incidents. In 2011, North Korea jammed South Korean GPS signals. In June 2017, Russia was suspected of spoofing the GPS signals of civilian shipping vessels in the Black Sea. In 2018, Symantec reported that a Chinese hacking group conducted cyberspace operations against satellite operators, infecting machines that control the satellites. In all three instances, there were no significant responses from the United States or the international community. However, none of these incidents occurred as part of an ongoing conflict or did they result in loss of life. "China-Based Hacking Breached Satellite, Defense Companies: Symantec," CNBC, June 19, 2018, https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html; Matt Burgess, "When a Tanker Vanishes, All the Evidence Points to Russia," *WIRED UK*, September 21, 2017, https://www.wired.co.uk/article/black-sea-ship-hacking-russia; Joe Gould, "Guided-Bomb Makers Anticipate GPS Jammers," *Defense News,* August 8, 2017, https://www.defensenews.com/air/2015/05/31/guided-bomb-makers-anticipate-gps-jammers/.

communications for fire support, medical evacuation, operational synchronization, or extraction would have limited options for quickly overcoming satellite denial, degradation, or destruction. High-frequency radio communication and line-of-sight radio relays require planning and preparation, and even when planned for, may require critical moments to establish communications. Even for a military accustomed to planning for redundant communications, satellite communications represent a significant vulnerability. The battlefield effects of disruption could include precious moments of complete isolation for dispersed units, failure of satellite reliant devices, and inaccuracy of precision fires.

How would U.S. forces respond to such battlefield disruption? Jamming of satellite signals is an expected condition of future battlefields for the U.S. military. Thus, the military response to battlefield jamming would likely be no different from the military response to any other standard battlefield action: employ new tactics or technology to counter the jamming.[85] The unknown is how the U.S. military, or the government as a whole, would respond to a cyberspace operation against U.S. satellites that achieves the same disruptive battlefield effects. While also somewhat expected on future battlefields, due to the ever-increasing paranoia of catastrophic cyberspace operations crippling critical national infrastructure, such an attack might trigger a significantly greater military or government response. A more significant response might also be expected due to the nature of a cyberspace operation compared to the nature of localized jamming of signals. While the battlefield effect may be the same, localized jamming does not require compromise of the critical, and expensive, space asset. A cyberspace operation likely would.

C. HOW DO BATTLEFIELD CYBERSPACE OPERATIONS IMPACT LAND FORCES? A KOREAN SCENARIO PART 1

Our thought experiment analyzes the battlefield impact of cyberspace operations through the lens of our Cyber Domain Interaction Framework. We conduct our analysis in the context of a hypothetical conflict on the Korean peninsula:

> Diplomacy with North Korea has ground to a halt. Harsh statements from the regime in Pyongyang force the United States to cancel planned

[85] Gould.

negotiations over denuclearization. Soon, multiple intelligence sources confirm that the DPRK is planning to deceive the United States. Even as North Korea dismantled the Punggye-ri test site, they began constructing new secret nuclear facilities. The U.S. president orders the DOD to present a military option for neutralizing North Korea's nuclear and ballistic missile capabilities.

The Joint Chiefs of Staff present a plan for a massive, synchronized operation to be executed in conjunction with the annual military exercises the U.S. conducts with South Korea. The plan is bold and risky. Successful execution hinges on the certain knowledge of locations of nuclear weapons and ballistic missiles within North Korea. The secretary of defense (SECDEF) orders U.S. Special Operations Command (USSOCOM) to conduct clandestine special reconnaissance missions into North Korea to confirm these locations. USSOCOM and Special Operations Command-Korea establish a combined joint special operations task force (CJSOTF) in a secret location near the demilitarized zone (DMZ) to execute the reconnaissance mission, primarily through South Korean special operations forces (SOF), intelligence assets, and former defectors handled by the South Korean National Intelligence Service. The CJSOTF is given six months to confirm the locations of nuclear weapons, facilities, and ballistic missiles to allow for final planning and rehearsals for the pre-emptive strike.

In this scenario, the CJSOTF has a unique role, providing critical information to enable the planning of a follow-on campaign that the commander of the United Nations, Combined Forces, and U.S. Forces Korea may not be able to obtain through other means. The DODIN provides the communications link between the task force, its reconnaissance teams, and higher headquarters through computer networks and satellite communications connections. Those data links facilitate mission planning, coordination, and execution; request and direct precision fire support to the task force; feed sensor inputs to operations centers and tactical units; and allow for data processing and analytics to be conducted across the DOD.

Soon after the establishment of the CJSOTF in South Korea, Chinese and North Korean intelligence assets in the country take notice. Within a month, they have infiltrated a contracting company that provides services on the base. Their assets gain physical access to a laptop that is connected to the classified system and installs malware. When any user logs into the laptop, the malware manipulates memory to send electromagnetic signals on cellular frequencies to a dedicated receiver hidden outside the building. The attacker, a well-known Chinese advanced persistent threat (APT) group, uses the link to gather critical operational information. They steal operations

> orders, concept briefs, personnel lists, logistics and communications plans and status, and much more. Within a couple of weeks, the Chinese APT has a thorough understanding of the CJSOTF's plan and scheme of maneuver for the reconnaissance operations. They pass the information to the North Koreans.

While a successful cyberspace operation like the one described in our scenario against classified U.S. military systems and networks may seem unlikely, due to the technical difficulty and coordination with national intelligence assets, it is not outside the realm of possibility. If such an attack were successful, would it be detected by U.S. forces? U.S. forces would likely detect the breach eventually, but detection of a cyberspace operation is difficult if the attack does not openly disrupt the operation of the system. As we have seen from our previous examples, detection typically has taken a long time. The OPM hack was stealing data for almost a year before being fully uncovered.[86] The Moonlight Maze hacks are believed to have remained undetected for about two years.[87] If we assume the U.S. military is twice as good at detecting attacks as the average civilian company, then we still have a planning factor of 103 days that the attacker could be in the system undetected.[88] That is more than three months of compromised operational information.

The difficulty in identifying malicious activity within a network has led to supplementing human defenders with advanced computer assets to support them. For example, the National Security Agency provided the Defense Information Security Agency with a platform called Sharkseer, which leverages artificial intelligence to monitor, and actively protect, the DODIN from advanced threats a human might not detect.[89] Would an advanced tool such as this be capable of protecting the networks of operational or tactical

---

[86] Brendan I. Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the U.S. Government," *WIRED,* October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[87] Doman, "The First Cyber Espionage Attacks."

[88] Luke Irwin, "How Long Does It Take to Detect a Cyber Attack?" *IT Governance USA* (blog), February 21, 2018, https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/.

[89] Justin Lynch, "The AI That Protects DoD Networks from Zero-Day Exploits," Fifth Domain, July 27, 2018, https://www.fifthdomain.com/dod/2018/07/27/the-ai-that-protects-dod-networks-from-zero-day-exploits/.

level military units, such as our notional CJSOTF? As illustrated by USCYBERCOM and JFHQ-DODIN's efforts to map and reorganize DOD's digital landscape, protecting the networks and systems of operational and tactical units is not only possible, but imperative.[90] By seeking to centralize and standardize the DODIN, software tools should be able to be used anywhere on the network. Network monitoring tools would monitor data in motion at critical points, such as the Internet access points and the JRSSs, while host-monitoring tools would monitor the behavior of the devices themselves.

Suppose attackers are successful at defeating these defensive tools. How would such compromise affect the task force's operations? With an estimated three months of undetected access to the CJSOTF's classified network, the DPRK forces would have active knowledge of unit composition and disposition; dates, times and locations of upcoming operations; logistics status, systems and processes; and potentially much more critical information. The battlefield potential of such knowledge in the hands of any enemy could be catastrophic. In our scenario, the reconnaissance missions would be compromised. They could be ambushed and destroyed, or reconnaissance targets could be staged, resulting in future operations targeting false or ambush-laden objectives. We believe it is a valid assumption within this scenario that such compromise of operational networks would likely result in mission failure for the CJSOTF. DPRK forces would eliminate South Korean intelligence assets. DPRK forces would also ambush and destroy or capture the U.S. and South Korean SOF Recon teams. North Korea would move as many of their nuclear facilities and ballistic missiles as possible after discovering the mission of the CJSOTF.

Attempts to discover the enemy's operational plans during wartime are as old as war itself. Knowing what the enemy will do while keeping them ignorant of friendly plans typically results in victory for the army with the information advantage. In this case, the compromise of an operational military network like the DODIN via cyberspace operations has historical parallels in codebreaking during World War II or the North Vietnamese double-cross of Military Assistance Command Vietnam-Studies and Observation Group

[90] Joint Chiefs of Staff, *Joint Communications System*, ix-x.

(MACV-SOG) secret agents. The Battle of Midway and the Battle of the Atlantic demonstrate the consequences such a cyberattack might have on combat, in that the clandestine interception of enemy operational information directly resulted in battlefield catastrophe for the unwitting opponent. The North Vietnamese double-cross of Central Intelligence Agency (CIA) and MACV-SOG secret agents is a direct historic parallel to our fictional Korean scenario. It demonstrates the effect a cyberspace operation could have on compromising human intelligence (HUMINT) assets in a theater of war and the potential to enable future military deception.[91]

> The CJSOTF prepares to infiltrate 10 three-man special reconnaissance teams consisting primarily of South Korean SOF. These teams will link up with intelligence assets in several provinces throughout the country via various insertion mediums. Each team has a list of targets: suspected locations of nuclear weapons, facilities, and ballistic missiles. They will report to the CJSOTF only during pre-planned communications windows, except in-extremis situations, using primarily satellite communications with high-frequency radio communications as an alternate. The CJSOTF plans to keep the teams in place throughout the entire operation, relying on the assistance of the intelligence assets to help hide and sustain them, and extract them only after the pre-emptive strike.
>
> The teams board small, unmarked planes, captured North Korean fishing junks, and allied submarines to begin their infiltration. They all meet a similar fate. One team conducts a high-altitude high-opening parachute jump into North Korea. They fly over 30 kilometers under canopy to their drop zone. As the operators land and begin to secure their equipment, spotlights blind them and machine gun and small arms fire blankets the drop zone. The operators take cover and attempt to report the contact to the CJSOTF and call for supporting fires. Their satellite radios are silent. The operators are killed or captured by the North Koreans within minutes before they can get their high-frequency radios into operation.
>
> Back in the operations center of the CJSOTF, the staff is getting nervous. Messages informing the CJSOTF that infiltration was successful should have come in by now. The commander and staff are beginning to fear something is wrong. After a few more minutes the messages start arriving, just a few pre-planned code words for each team informing the CJSOTF that infiltration is complete.

---

[91] Richard H. Shultz, The Secret War against Hanoi: Kennedy's and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam, (New York: HarperCollins, 1999), 90–93.

The undetected compromise of operational information resulted in the destruction of all of the reconnaissance teams in the scenario. While the scenario contemplates compromise before the infiltration of the teams, even if the compromise had occurred later in the mission the result would be the same. The DPRK would know where the teams were hiding, where they were going, and who was on them. They would simply have set ambushes elsewhere and then moved all of their nuclear weapons and ballistic missiles to ensure that the follow-on strike would miss its targets.

Something else happened in this scenario besides just the compromise of the CJSOTF's classified networks. When ambushed, the reconnaissance team's satellite communications did not work. Significant reliance on satellites for communications in North Korea is very realistic. The United States has no communications infrastructure above the 38th parallel, with the possible exception of ships off the coast or planes in the air to serve as relays for line-of-sight communications. Aircraft would probably be the only viable option for line-of-sight relay due to the rugged terrain, and no aircraft could fly above the 38th parallel in support of this reconnaissance mission due to the significant amount of anti-aircraft assets in North Korea and the political risk of flying any aircraft over North Korea in support of clandestine or covert operations.[92] Perhaps the intelligence assets could have set up relays on mountaintops, but this would still be an unlikely and unreliable option. In our scenario, the failure of the satellite communications radios reflects the North Korean capability to jam the signals locally or even hack the satellites themselves.[93] In this case, the DPRK planned the ambushes to be the first step in a larger strategic deception: eliminating the CJSOTF reconnaissance capability while having them think it was successful in executing its mission. This deception was made possible by the compromise of the classified network as well as the cyberspace operations conducted

---

[92] Anthony H. Cordesman and Charles Ayers, *The Military Balance in the Koreas and Northeast Asia* (Washington, DC: Center for Strategic International Studies, 2016), 124, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161121_korea_book_2016.pdf.

[93] The threat from satellite hacking is rising in prominence, as evidenced in the Office of the Inspector General's findings of vulnerabilities in NASA computers that control spacecraft. Jason Fritz, "Satellite Hacking: A Guide for the Perplexed," *Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013): 30–31.

against the satellites themselves, allowing the North Koreans to send the CJSOTF the exact messages they expect to receive.

D. CONCLUSION

While this scenario emphasized the clandestine infiltration of the CJSOTFs' classified network, cyberspace operations could also be used to disrupt the same network.[94] The scenario illustrated this when satellite communications were disrupted during the ambushes of the reconnaissance teams. How would a disruptive cyberspace operation against the DODIN differ from a non-disruptive one? A disruptive attack on the DODIN would have an immediate noticeable impact on the network, whereas detecting clandestine infiltration relies on finding anomalies that were designed to go unnoticed. The results of a disruptive cyberspace operation would be readily apparent as the network itself would have to be noticeably affected to achieve the desired battlefield effect.

How would such attacks affect CJSOTF operations? The effects of these attacks are inherently temporary. Even assuming the disruptive attack renders a technological capability such as satellite communication permanently useless, maneuver units would quickly adapt and find a way to continue operations. Whether that adaptation would be switching to an alternate communications system, operating autonomously but guided by the intent of the commander in lieu of orders, or simply fixing or replacing the damaged system, deployed forces will continue the mission. The scenario illustrated this adaptive behavior during the ambush of the reconnaissance teams. The teams recognized the failure of satellite communications and attempted to employ high-frequency radios, but the DPRK forces killed or captured them before they could.

Additional key differences between disruptive cyberspace operations and clandestine cyberspace operations are worthy of note. First, due to the temporary nature of disruption, timing and synchronization with terrestrial operations are critical. Yet it is also difficult. For disruptive cyberspace operations to be synchronized with terrestrial operations, the attacker would need to have successfully compromised a system—and

[94] For simplicity, we include the effects of disable, degrade, and deny all under the term "disrupt."

remain undetected until it was time to execute—with a sophisticated payload that could be executed either by remote control or at a programmed time. This is hard enough to accomplish against a relatively unprotected civilian system; the difficulty increases considerably when considering encrypted, air-gapped, or frequency-hopping military systems.

Second, gaining entry into a system typically uses the same tools and methods, regardless of the purpose of the payload. The "cyber kill chain" highlights this point perfectly, as the exploits used to gain access could be the same despite one payload encrypting data while another payload establishes a reverse shell connection to an attacker.[95] Additionally, upon the discovery of a cyberspace vulnerability, it is typically quickly patched, rendering that cyber weapon potentially useless against the target system.[96] Therefore, conducting a disruptive cyberspace operation potentially wastes a valuable exploit that could have been used to gather operational information over an extended period of time. It will be up to the joint force commander to decide upon the more effective use of his arsenal of cyber weapons.

Contrasting the differences between disruptive cyberspace operations and clandestine cyberspace operations highlights an important conclusion. Clandestine cyberspace operations that seek to infiltrate systems and gather operational information are likely to prove a more efficient use of offensive cyberspace operations on the battlefield. This is a function of both the difficulty of synchronizing disruptive cyberspace operations with terrestrial military operations, and the inherently short duration of their resulting effects. Considering that software vulnerabilities are typically quickly patched once discovered, disruptive battlefield cyberspace operations should be considered carefully and used sparingly.

---

[95] In the weaponization phase of the Cyber Kill Chain, an exploit is paired with a payload in preparation for an attack. "Gaining the Advantage: Applying the Cyber Kill Chain Methodology to Network Defense," Lockheed Martin, 2015, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

[96] Benjamin Jensen and David Banks, *Cyberspace Operations in Conflict: Lessons from Analytic Wargames* (Berkeley, CA: Center for Long Term Cybersecurity, April 2018), 18, https://cltc.berkeley.edu/2018/04/16/cyber-operations-conflict-lessons-analytic-wargames/.

Electronic warfare or physical attacks on military communications networks would be a better means for achieving disruptive effects. These capabilities do not have limited uses like cyber weapons; they can be employed quickly, easily, and reliably time and again to disrupt enemy communications on the battlefield, and they are easier to synchronize with other physical military operations. Thus, a commander should not conduct disruptive cyberspace operations opportunistically, especially if a physical or electronic warfare alternative is available and could achieve the same effects.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THOUGHT EXPERIMENT—PART II

A. INTRODUCTION

Part I of our thought experiment observed the potential impact of cyberspace-based operations on SOF conducting clandestine reconnaissance operations prior to open conflict on the Korean peninsula. It ended with the destruction of the reconnaissance forces as a result of undetected infiltration of U.S. classified computer networks and the beginning of a North Korean military deception. Part II envisions the impacts of cyberspace operations on the United States' attempts to flow forces into the theater and engage in high-intensity combat.

B. HOW DO BATTLEFIELD CYBERSPACE OPERATIONS IMPACT LAND FORCES? A KOREAN SCENARIO PART 2

> As a result of clandestinely stealing data from the CJSOTF classified computers, the North Koreans have a good idea of the coalition plan for a pre-emptive strike. They know the strike is planned to coincide with the annual exercises conducted between the United States and South Korea, but they do not know the exact date or all of the units that will enter the country for the operation.
>
> In an attempt to disrupt or delay the United States' ability to flow forces into the theater, North Korean cyberspace operators attack the U.S. transportation system TC-AIMS II. They gain access by spear-phishing to compromise a user's machine and install a remote-access tool. When the user logs into TC-AIMS II through the web-based interface, the attackers insert malware directly into the TC-AIMS II system. The malware specifically targets its databases with the intent of disrupting the deployment of U.S. forces to the Korean peninsula. The malware is scripted to execute at a set date and time. Two months before the start of the joint exercises, it activates a modified version of the infamous Shamoon malware and wipes thousands of hard drives and servers across the DODIN containing TC-AIMS II data, replacing it with Islamist propaganda.
>
> North Korea edited the malware to ensure success against a DOD target, considering the target operating system version and patches, leaving as many forensic clues as possible that point to Iran as the culprit. Considering the ongoing conflicts in Syria and Yemen, the U.S. intelligence community has ample reason to suspect Iran for the hack, leaving the United States

> unsuspecting of the compromise of the CJSOTF systems and North Korean knowledge of the impending coalition strike.
>
> The U.S. logistics system scrambles to recover, replacing hardware and re-creating the databases and load plans from hard copies and backups. The cyberspace operation causes chaos for U.S. deployments globally, not just to Korea, which adds to the likelihood of misattribution to Iran. Flights and ships destined for the Korean peninsula are delayed by days, some even for weeks, as U.S. logisticians are forced to re-create plans and produce the required shipping forms and paperwork manually. As a result of this unforeseen disruption, the coalition commander decides to shift D-Day a week later than originally planned.

Could a U.S. adversary conduct a cyberspace operation against critical logistics and transportation systems? While some critical deployment planning systems reside on the classified network, TC-AIMS II is a primary source for transportation management that operates on the unclassified network.[97] It is an integrator system that takes deployment data and translates it into load plans for planes, ships, trucks, and trains. While the DODIN is a well-protected network, the unclassified NIPRNET still connects to the Internet and TC-AIMS II is accessible from a web-based portal page. Thus, attacks against systems or services on the NIPRNET are much more likely to be successful than attacks against the classified networks. Perhaps that is why the 2003 supportability strategy for the TC-AIMS II system identified cyberspace operations as among the most significant threats to the system.[98]

If an adversary successfully damaged unit deployment systems and databases, how much would it impact the U.S. military's ability to project force to the Korean peninsula? The Shamoon malware not only serves as a useful deception in our scenario but is also a prime example for gauging the amount of potential damage destructive malware could cause to U.S. logistics and transportation systems. Shamoon was designed to destroy stored data and corrupt the master boot record of infected machines, forcing hardware components

---

[97] Defense Acquisition University, "Supportability Strategy for the Transportation Coordinators' Automated Information for Movement System II" (Washington, DC: Defense Acquisition University, March 2003), 3, 10, https://www.dau.mil/cop/log/DAU%20Sponsored%20Documents/Supportability%20Strategy%20for%20TC%20AIMS%20II%20DTD%20March%202003.pdf.

[98] Defense Acquisition University, 11.

to be replaced to restore network operations.[99] In 2012, Shamoon destroyed tens of thousands of hard drives and forced Saudi Aramco to shut down their network temporarily.[100] In 2017, five years after the first appearance of the malware, a second variant of Shamoon destroyed computers and disabled networks of 15 Saudi Arabian government agencies.[101]

Shamoon illustrates a recurring problem in cybersecurity, that despite patching known vulnerabilities, old malware continues to present a threat. There are numerous other examples of recycled malware to add to the Shamoon example. Other prominent examples of malware being reused years later include the Seasalt-Oceansalt malware used by APT 1, which reappeared after a five-year hiatus, and the code for the Reaper Botnet, which was modified and used in the Mirai Botnet.[102] This is representative of the cat and mouse game that is cyberspace operations. The attacker finds a vulnerability, develops an exploit, pairs it with a payload, and executes. The defenders then patch the vulnerability and use the signatures of the malware to improve detection. The attacker responds by finding a new vulnerability, developing a new exploit, modifying the old payload, and then executing again. The signatures used to detect the old malware are potentially useless even with only minor changes to the code, and due to the impossibly complex nature of modern software, vulnerabilities will almost certainly always exist.

Our scenario envisions a similar limited duration disruption of computer and network-based resources that facilitate U.S. military forces transportation into the theater. The key to mitigating an attack like Shamoon is more than just crafting better means of

---

99 "Shamoon/DistTrack Malware (Update B)," ICS-CERT, accessed September 14, 2018, https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B.

100 Nicole Perlroth, "Cyberattack on Saudi Oil Firm Disquiets U.S.," *New York Times*, October 23, 2012, sec. Global Business, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

101 Ms. Smith, "Saudi Arabia Again Hit with Disk-Wiping Malware Shamoon 2," CSO Online, January 24, 2017, 2, https://www.csoonline.com/article/3161146/security/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html.

102 Brian Barrett, "The Mysterious Return of Years-Old Chinese Malware," *WIRED*, October 18, 2018, https://www.wired.com/story/mysterious-return-of-years-old-chinese-malware-apt1/; "What's Old Is New Again: Why Hackers Reuse Malware," Secplicity, November 21, 2017, https://www.secplicity.org/2017/11/20/whats-old-new-hackers-reuse-malware/.

detecting old malware; it is the ability of an organization to recover from the attack and resume operations as quickly as possible.[103] It took Saudi Aramco five months to recover from the 2012 attack.[104] They were forced to make emergency purchases of replacement computer hardware and conduct business administration processes manually or by fax machine.[105] Despite the slow recovery of Saudi Aramco's information technology systems, their oil production was not affected. The systems that controlled operations were separate from the internal networks of the company.[106] However, every unit in the U.S. Army uses TC-AIMS II for planning and executing unit movement operations.[107] A Shamoon-like attack could be expected to slow or degrade operations temporarily until workarounds, such as manually created load plans, were established.

If we assume the U.S. military could recover in half the time it took Saudi Aramco, then in our scenario the disruption to U.S. deployments could still last for months. We take into consideration, however, that the shock value of attacks like Shamoon has decreased since 2012, and we assume large organizations, especially the U.S. military, are more prepared to respond. As a result, in our scenario we calculate the impact of the disruption as delaying troop deployments for just one week, which could still be critically important.

> Reports begin to spread through the intelligence services of various governments regarding the disruption of the U.S. military's logistics systems. Similar disruptive cyberspace operations are reported to be targeting major international air and maritime shipping hubs. The press is openly discussing the attacks against the U.S. military and global transportation systems, while the pundits begin to speculate on the culprit of such an attack.

---

103 Recover is the fifth function of the NIST Cybersecurity framework core. Our scenario assumes that cyber defense failed, highlighting the importance of a pre-planned and resourced ability to recover. "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," National Institute of Standards and Technology, April 16, 2018, 8, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

104 Jose Pagliery, "The Inside Story of the Biggest Hack in History," CNNMoney, August 5, 2015, https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

105 Pagliery.

106 Pagliery.

107 Department of the Army, *Army Deployment and Redeployment* ATP 3–35 (Washington, DC: Department of the Army, March 2015), 1–3, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6984_ATP%203-35%20C1%20INCL%20FINAL%20WEB.pdf.

North Korea uses the window they created to launch a pre-emptive strike against South Korea. North Korean SOF spent the weeks prior to D-Day penetrating South Korea through a series of pre-established entry points. At H-Hour, the designated time of the attack, North Korean SOF execute sabotage operations in a series of attacks against South Korean bridges, airports, and seaports, as well as strikes against key military leaders. The special operations in South Korea are intended to delay the military's response to North Korean attacks along the DMZ and further delay efforts by the United States to flow forces into the Korean peninsula.

Also at H-Hour, North Korea launches offensive cyberspace operations against civilian communications and military command and control targets. They conduct denial of service attacks against commercial and government web-based communications services within South Korea. They also launch a cyberspace operation against Seoul's power grid in a move very reminiscent of the cyberspace operations that caused blackouts in Ivano-Frankivsk region of Ukraine in 2015.[108]

Finally, North Korea disrupts allied military satellite communications services, specifically in the vicinity of command and control nodes along the DMZ. These operations are focused on disrupting the flow of information in Seoul and along the DMZ to prevent allied forces from mounting a quick response to the North Korean strike. The temporary loss of most means of communication results in the effective isolation of allied forces as artillery fire begins to fall.

In conjunction with the SOF strikes and cyberspace operations, North Korea begins employing artillery fires from their hardened positions North of the DMZ. The artillery barrage is not intended to damage the city of Seoul, but to isolate it. Artillery targets include allied military command centers, headquarters, communications infrastructure, motor pools, and civilian infrastructure such as the roads and bridges linking Incheon International Airport with Seoul. The combination of cyberspace operations against satellite communications, Internet service providers and cellular service providers, as well as conventional artillery bombardment of allied command and control nodes, causes significant damage and ultimately delays a coordinated allied response to the attack.

As the first artillery rounds begin to land south of the DMZ, two large North Korean assault echelons conduct a series of penetrations in order to break through South Korean defenses. An armored force attacks along the eastern coastal road to capture Sokcho and Gangneung. This attack is a feint designed to convince the allies that North Korea's objective is to seize the entire peninsula. Battalion-sized feints are launched at locations all along the DMZ to add to the confusion of allied forces and fix defending forces in place. Concurrently, North Korean forces conduct a combined arms penetration across the DMZ north of Seoul. They execute a series

[108] "Hackers Caused a Blackout for the First Time, Researchers Say," *Washington Post*, November 14, 2018, https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/.

of highly choreographed breaches that penetrate allied lines and create avenues of approach for North Korean armored columns and mechanized forces. The fighting is brutal as both sides execute plans that have been trained and rehearsed for decades, yet the allies are at a temporary disadvantage. Air support is slow to arrive, delayed for hours due to disruptions in allied communications, and supporting fires from aircraft, ground, and naval assets are minimal and inaccurate as allied forces struggle to coordinate fire and maneuver. Speed is the critical factor, as North Korea has to take full advantage of the element of surprise and the degradation of U.S. and South Korean communications, command, and control.

Once the North Korean forces break through the DMZ, their mechanized forces leverage the South's well-developed road system to lead a drive on Seoul. With the preponderance of military forces arrayed along the DMZ, no military forces of significant size to halt the North Korean advance are stationed within the city and police forces cannot hope to stop the attack. Enemy tanks and armored vehicles push civilian traffic off the road as they sprint to seize objectives in the city center and throughout heavily populated sectors of the city. Infantry forces establish checkpoints at key intersections in an effort to stem the flow of people fleeing the city and increase the deterrent to an allied counterattack. Within 12 hours of the operation's beginning, North Korean forces seize key portions of northern Seoul.

During the first hour of the attack, the North Koreans leverage their Chinese and Russian partners to conduct an international diplomatic offensive. They provide stolen plans and communications that detail the allied reconnaissance into North Korea and the planned allied strike to media outlets worldwide. Kim Jong Un, with Russian and Chinese support, appeals to the international community to condemn illegal U.S. actions and portrays his highly restrained response as necessary for the defense of North Korea. Once Seoul is surrounded and partially occupied, he calls for a ceasefire and the establishment of an international commission to arbitrate the end of the war. Kim Jong Un wants full international recognition of North Korea as a sovereign nation, recognition of the legitimacy of his nuclear program, and lifting of economic sanctions. His bargaining chip is Seoul. He offers to return all occupied territories to South Korea in exchange for his demands. He highlights North Korean restraint, specifically their non-use of ballistic missiles and weapons of mass destruction during the offensive, as well as their relatively retrained approach to Seoul. Kim pledges North Korea will maintain such civilized restraint as long as the United States and South Korea refrain from invading the North.

Fighting continues over the next 24 hours while North Korea pushes more forces into parts of the city. By H+36, approximately 150,000 North Korean troops surround or occupy portions of Seoul. DPRK troops establish defensive positions in and around Seoul ranging from the city center north to the outer edges of the vast urban sprawl. Borrowing from Egyptian strategy in the 1973 Yom Kippur War, North Korea's military shifts to a strategic defensive underneath an air-defense and anti-ship missile umbrella, establishing strongpoints in Seoul, SokCho, and Gangneung.

Could North Korea successfully conduct offensive cyberspace operations against Internet and cellular service, U.S. satellite communications, or the Seoul power grid? North Korea has already demonstrated its intent, if not yet the capability to target South Korean energy infrastructure. In December 2014, North Korea launched an unsuccessful cyberattack against Korea Hydro and Nuclear Power designed to steal data and damage computers.[109] A year prior, North Korean cyberspace operators conducted damaging attacks against banks and public media companies employing malware that wipes master boot records, a tactic similar to that used against Saudi Aramco. Also in 2013, North Korean hackers conducted denial of service attacks against government and media websites as well as domain name servers.[110] Therefore, we assess that North Korea does have the capability to conduct offensive cyberspace operations against civilian websites, companies, and infrastructure. The effects envisioned in our scenario are at least possible, though perhaps unlikely to be synchronized so precisely with ground operations for now.

As discussed briefly in the previous chapter, we also assume that North Korea does have the ability to disrupt U.S. satellite communications in the region. The most likely means of disrupting satellite communications would probably be electromagnetic jamming rather than cyberspace operations. However, cyberspace operations can achieve similar effects. At the Black Hat 2018 cybersecurity conference, security researcher Ruben Santamarta gave a presentation on satellite hacking where he claimed he could control antenna position and power usage on military and maritime satellites.[111] Such control could enable a hacker to produce disruptive effects similar to those envisioned in our scenario.

If the cyberspace operations envisioned in our scenario were successful, how would they affect allied forces? North Korean offensive cyberspace operations against Internet and cellular service providers would seek to disrupt civilian communications within Seoul. The purpose would be similar to that which was evident in the Russian invasion of Georgia.

---

[109] Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats," July 25, 2016, 24, http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf.

[110] Boo, 24.

[111] Max Eddy, "Satellite Communications Hacks Are Real, and They're Terrifying," PCmag, September 22, 2018, https://www.pcmag.com/news/363004/satellite-communications-hacks-are-real-and-theyre-terrify.

Coordinated cyberspace operations disrupted government and civilian communications throughout the country in a two-pronged effort to slow internal responses and confuse international opinion. A combination of distributed denial of service attacks (DDoS) against Internet service providers (ISP) and Domain Name System (DNS) service providers, as well as electromagnetic jamming of cellular towers in Seoul, could likely achieve the communication disruption envisioned in our scenario. When coupled with potential blackouts as a result of attacks on the power grid, public communication in Seoul could be disrupted for hours, resulting in confusing, inaccurate, or late reporting on events occurring in Seoul.

The cyberspace operations against allied satellite communications would produce a denial-of-service effect, whether through downlink or uplink jamming or control of the antenna. During Operation Iraqi Freedom, the U.S. military relied heavily on commercial satellite communications and experienced numerous cases of degraded or terminated satellite communications between July 2004 and November 2005. Twenty-one of those cases were considered as potentially due to jamming from a hostile actor with an average duration of 85 hours per event. In 2011, North Korea jammed GPS signals in South Korea along the DMZ for 10 days while the U.S. and South Korea were conducting annual military exercises.

Our scenario incorporates cyberspace operations against allied satellite communications as one piece of a coordinated assault on allied command, control, and communications. More importantly, the cyberwar assault is synchronized with the terrestrial military force required to take advantage of the fleeting opportunity provided by disrupting allied communications. As noted in the previous chapter, military forces will eventually adapt and overcome disruption. The effects will be temporary even if they last for hours or days. Therefore, precise synchronization with physical maneuver forces is critical to the successful use of disruptive cyberspace operations to achieve battlefield objectives.

> The coalition quickly realizes the limited nature of Pyongyang's attack. Coupled with the high-visibility diplomatic pressure, U.S. and South Korean responses are restrained. The allies maintain control of the major ports and airfields in South

Korea and U.S. transportation systems have recovered from North Korean cyberspace operations as a result of the work of JFHQ-DODIN and cyber protection teams identifying, isolating, and removing the malware from U.S. systems. U.S. ground forces begin to flow into the country unchallenged. With North Korean ground forces dug into defensive positions in and around Seoul, Sokcho, and Gangneung, allied ground forces prepare for tough urban combat.

The recapture of Gangneung and Sokcho takes two weeks. The U.S. and South Korean forces liberate the cities, though allied and civilian casualties are uncomfortably high. The fighting in these two cities gives only a glimpse of the difficulty to come in freeing Seoul.

Allied armored brigades strike to the north of Seoul first, cutting off lines of communication to North Korea while air and sea power deliver punishing fires to air defense and artillery targets supporting the forces in Seoul. USCYBERCOM and JFHQ-DODIN have deployed additional cyber defense teams to support U.S. Forces Korea, and within two weeks, they have identified and corrected the intrusions in the CJSOTF systems and U.S. satellites. As the U.S. high-tech war machine is finally operating at full capacity, prospects look dim for the North Koreans.

Kim's gamble is that the price to dig North Korean forces out of Seoul street by street is too high for the United States and South Koreans to pay. The allies call his bluff, betting that he will not escalate to nuclear use in extremis. Once Seoul is isolated from resupply and supporting fires, mechanized and light infantry, supported by dispersed armor companies and attack aviation, begin the herculean effort to clear the city methodically. Prior to the assault to assist in developing greater situational awareness within the city, cyberspace operations map the computer networks in the city, establish communications and reporting channels with trapped residents, and gain access to Internet-connected sensors and civilian infrastructure.

The coalition operations center monitoring the cyberspace operations is soon receiving reports of unit compositions and dispositions throughout the city, complete with pictures taken by a smartphone and uploaded to their reporting websites. Weather, traffic, and security cameras throughout the city provide live feeds of key intersections and locations. Enemy positions are populated on the common operating picture shared by all allied ground units and live video feeds are accessible via smartphone. Coalition forces leverage this information superiority to great effect, avoiding multiple ambushes and surprising their North Korean adversaries repeatedly. However, knowledge of the battlefield is never perfect, or even complete, and the fighting is hard. Coalition and civilian casualties are high, but the city is eventually retaken.

Could U.S. tactical forces conduct cyberspace operations in support of combat in a dense urban environment? Most of the cyberspace operations described in our scenario are

far simpler than some of the highly sophisticated operations the U.S. government is believed to have executed.[112] Many Internet-connected devices are vulnerable as most arrive with default passwords that many users do not change.[113] Hacking closed-circuit television (CCTV) feeds might be more challenging. However, a software vulnerability discovered recently was estimated to have put over 100,000 CCTV camera installations worldwide at risk of compromise.[114]

The U.S. military undoubtedly has the skilled personnel within USCYBERCOM and the service cyber commands to conduct these types of operations, but tactical formations such as the brigade combat team do not have organic cyber assets.[115] USCYBERCOM announced in May 2018 that the Cyber Mission Force had reached full operational capability.[116] The Cyber Mission Force consists of national mission teams, which support national objectives in cyberspace, and combat mission teams, which support geographic combatant commander objectives in cyberspace.[117] Additionally, U.S. Army cyber command has three Expeditionary Cyber Support Detachments designed to embed with tactical units.[118]

---

112 "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *WIRED*, accessed May 11, 2018, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

113 The Mirai botnet was one of the first examples that demonstrated the simplicity of IOT hacking. Andy Greenberg, "The Reaper Botnet Has Already Infected a Million Networks," *WIRED*, October 20, 2017, https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

114 "Critical RCE Peekaboo Bug in NVR Surveillance System, PoC Available," BleepingComputer, accessed September 20, 2018, https://www.bleepingcomputer.com/news/security/critical-rce-peekaboo-bug-in-nvr-surveillance-system-poc-available/.

115 However, U.S. Army Cyber Command has built cyber detachments designed to support at levels of corps and below. Todd South, "The Army Is Putting Cyber, Electronic Warfare Teams in Its BCTs," *Army Times,* February 20, 2018, https://www.armytimes.com/news/your-army/2018/02/20/the-army-is-putting-cyber-electronic-warfare-teams-in-its-bcts/.

116 "Cyber Mission Force Achieves Full Operational Capability," U.S. Cyber Command, accessed September 20, 2018, http://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/.

117 U.S. Cyber Command.

118 Mark Pomerleau, "Army Looks to Build Stronger Tactical Cyber Teams," Fifth Domain, September 14, 2018, https://www.fifthdomain.com/dod/army/2018/09/14/army-looks-to-build-stronger-tactical-cyber-teams/.

Conflict in Korea would be a main effort for the DOD, and at the very least, we would assume that multiple combat mission teams, and perhaps a national mission team as well, would be made available to the commander of U.S. Forces Korea. We also assume that U.S. Army Cyber Command would provide expeditionary cyber support detachments. In our scenario, we envision the U.S. Forces Korea Commander employing cyber assets in support of ground combat in Seoul, providing redundant cyberspace operations capability from at least the brigade level to up to U.S. Forces Korea.

How would cyberspace operations affect combat in large, dense cities? The U.S. Army has spent a considerable amount of time thinking about the megacity problem, under the assumption that fighting in megacities will be unavoidable in future conflicts.[119] The vast majority of responses to a survey conducted by the Army's Mad Scientist Initiative calling for ideas to help address the problem of fighting in a megacity revolved around how to increase situational awareness in the megacity environment.[120] Many of these ideas captured opportunities provided by cyberspace as a result of the growing Internet of Things and ubiquitous connectivity offered in highly developed megacities.

Every megacity should be analyzed and considered separately.[121] In the specific context of Seoul, cyberspace opportunities for increasing situational awareness seem very plausible. South Korea, and especially its capital, is a nation and a culture that embraces high technology. Seoul is a city with developed infrastructure, stable governance, and a tech-savvy population. The city is teeming with wireless networks and Internet-connected devices and

---

[119] Marc Harris et al., "Megacities and the U.S. Army: Preparing for a Complex and Uncertain Future" Chief of Staff of the Army Strategic Studies Group, June 2014, 4–5, https://www.army.mil/e2/c/downloads/351235.pdf.

[120] David N. Farrell and Megan Ward, *Megacities and Dense Urban Areas Initiative: Data Collection and Analysis,* 16–2955 (Washington, DC: MITRE, 2016), 14, https://www.mitre.org/sites/default/files/publications/16-2955-tradoc-g-2-mad-scientists-megacities-analysis.pdf.

[121] Gian Gentile et al., *Reimagining the Character of Urban Operations for the U.S. Army: How the Past Can Inform the Present and Future* (Santa Monica, CA: RAND, 2017), 17, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1602/RAND_RR1602.pdf.

sensors.[122] In our scenario, cyberspace operations are used to gain access to these flows of information provided by sensors throughout the city such as CCTV networks, traffic cameras, and weather cameras.

The heightened situational awareness for allied forces is in stark contrast with the lack of situational awareness for North Korean forces, due to the assumed lack of technological familiarity among average North Korean troops. While North Korea boasts an impressive cyberspace operations capability, based on their penchant for strategic use we assume this capability would not be integrated with tactical forces.[123] Additionally, North Korea is a nation where access to the Internet is highly controlled.[124] We therefore assume that average North Korean troops will be unfamiliar with the Internet in general, and specifically smart devices and the Internet of things.

Also crucial to the specific analysis of Seoul is the attitude of the population toward the military forces operating within the city. One of the most significant reasons the U.S. Army fears megacity combat is the assumption of an unsupportive population.[125] However, in our scenario, the South Korean people would welcome allied forces as liberators after being occupied by North Korean forces. They would likely seek to assist them where possible and perhaps even organize organic resistance against the North Korean occupiers. It is this envisioned popular support within Seoul that part of our cyberspace operations taps into, by establishing means through cyberspace for individuals in Seoul to communicate tactically relevant information to allied military forces. This unique characteristic of combat in Seoul makes the situation far different from recent historical parallels of urban fighting in Baghdad, Fallujah, or Grozny. While the dense urban terrain and aversion to collateral damage would

---

[122] Frances Cha and Lucy Corne CNN, "50 Reasons Why Seoul Is World's Greatest City," CNN Travel, July 12, 2017, https://www.cnn.com/travel/article/50-reasons-why-seoul-worlds-greatest-city/index.html; "Is Seoul the World's Smartest City?," *ReadWrite* (blog), May 12, 2016, https://readwrite.com/2016/05/12/is-seoul-the-worlds-smartest-city-ct1/.

[123] Emma Chanlett-Avery et al., *North Korean Cyber Capabilities: In Brief,* CRS Report No. R44912 (Washington, DC: Congressional Research Service, 2017), 1–2, 4–8, https://fas.org/sgp/crs/row/R44912.pdf.

[124] Chanlett-Avery et al., 1–2.

[125] As illustrated by case studies analyzing combat in Mogadishu, Grozny, and Baghdad. None of these case studies evaluated combat in urban terrain with a populace supportive of the military operations. Gentile et al., "Reimagining the Character of Urban Operations for the U.S. Army," 28, 41–42, 47–48.

limit the use of U.S. and South Korean long-range precision fires, the supportive civilian population, high-tech infrastructure, and widespread Internet connectivity would create opportunities for improving situational awareness and provide networked communication through cyberspace operations.

C. CONCLUSION

Part II of our thought experiment saw cyberspace operations used by North Korea to create temporary disruption of allied communications, command, and control capabilities. Allied forces, on the other hand, used cyberspace operations in a technologically advanced, dense urban environment to enhance their situational awareness waging what Martin Libicki has called "intelligence-based warfare." In line with our cyber domain interaction framework, both belligerents used cyberspace operations to attack two specific technological capabilities tied to the cyber domain: global communications networks and sensor networks. By attacking these capabilities, they manipulated the effects those capabilities manifest on the battlefield: instant global communications were disrupted for hours in conjunction with a multi-pronged combined arms assault, and situational awareness for ground forces in Seoul was enhanced by tapping into Internet-connected video feeds.

What emerges from an analysis of North Korean cyberspace operations to disrupt allied communications is that synchronization of cyber operations with the ground assault is a necessary condition for success. Many experts have discussed the need for and difficulty of synchronizing cyberspace operations with terrestrial operations for them to have any meaningful battlefield effect. A recent study aimed to demonstrate the battlefield impact of cyberspace operations concluded that cyberspace operations have no observable effect on battlefield actions. However, the authors note in these instances the lack of coordination between cyberspace operations and ground operations, likening it to the often poor coordination between air power and ground forces in World War I. Additionally, the authors excluded the Russo-Georgian War of 2008, the best-known case of synchronized physical and cyberspace operations, from their study.

Our thought experiment highlights the critical role synchronization plays when using cyberspace operations to create disruptive battlefield effects. In this scenario, North Korean

deception after discovering allied plans for a pre-emptive strike enabled a surprise attack on South Korea. However, the ironically named DMZ is perhaps the most heavily armed place on the planet. The United States and South Korea have considerable military assets stationed there, but quantitatively their forces are dwarfed by those of North Korea. The allies make up for lack of numbers with higher-quality and cutting-edge technology, including the ability to bring overwhelming fire swiftly to bear on any North Korean assault. By disrupting allied communications, the DPRK disabled the United States' and South Korea's ability to direct ground maneuver or leverage their long-range precision fires quickly enough to prevent North Korea's seizure of parts of Seoul; but that disruption would likely have been ineffective if it were an hour too early or an hour too late.

An analysis of allied cyberspace operations to enhance situational awareness within Seoul highlights the contrast between conducting cyberspace operations against civilian systems connected to the Internet and military systems that may or may not be connected to the Internet: civilian systems connected to the Internet are significantly easier to breach. It also highlights the importance terrain may play regarding the opportunities that might be available through cyberspace. While the terrain of Seoul limits the value of standard military airborne and satellite surveillance or reconnaissance assets, the highly developed and high-tech nature of the city provides numerous cyberspace opportunities to enhance situational awareness that would be unavailable elsewhere.

This idea may seem counterintuitive. While it is true that cyberspace may be accessible from anywhere with the proper technology, physical terrain still does matter, especially in the context of planning a military campaign. The connectivity of the physical terrain within which military operations will be conducted is important in determining what potential cyberspace operations are available to support a course of action. Perhaps more importantly, physical terrain may sometimes constitute key terrain for cyberspace operations. Such key terrain might be Internet exchange points, physical routers or servers, cellular towers, power plants, electrical substations, undersea cables, or other targets. As was demonstrated by the Operation Desert Storm air campaign's targeting of Iraqi command and control capabilities, affecting physical targets that represent key terrain in cyberspace is often

easier in the physical domains than through cyberspace.[126] Physical attacks, as opposed to cyberspace operations, to create disruptive battlespace effects are also more easily synchronized with terrestrial military operations, as conventional military forces and weapons would accomplish the attack.

Our two-part thought experiment has attempted to envision a diverse set of cyberspace operations deliberately aimed at creating battlefield effects, with the intent of exploring the feasibility of such actions as well as their impacts on maneuver warfare. In the next section, we evaluate the insights provided by the thought experiments and analyze their implications for modern warfare.

[126] The U.S. air campaign in Operation DESERT STORM targeted Iraqi command and control capabilities prior to the ground campaign. While Iraqi command and control might not have been facilitated through cyberspace, the U.S. air campaign in the gulf war designating physical targets to degrade command and control capabilities mirrors the idea of targeting physical key terrain that sustains cyberspace. Charles A. Horner, "The Air Campaign," *Military Review* LXXI, no. 9 (September 1991): 24–25.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS AND CONCLUSION

A. INTRODUCTION

In this thesis, we have attempted to envision how cyber operations may affect the modern battlefield in order to identify what the cyber domain implies for land warfare. We noted that the bulk of the conversation that has taken place over the past few decades has primarily focused on the strategic implications of this new domain, rather than what it implies for ground forces in combat. Given the lack of available historical case studies to analyze, we conducted a two-part thought experiment to visualize cyberspace operations conducted as part of a possible future military conflict on the Korean peninsula.

We created a theoretical framework for envisioning the interaction between the cyber domain and the physical domains. Our framework identified four primary technological capabilities that rely on cyberspace to create multiple battlefield effects for modern militaries. Those four capabilities are global communication networks; sensor networks; data processing, storage and analytics; and artificial intelligence. The effects these capabilities enable on the battlefield include, but are not necessarily limited to, long-range precision fires, empowered small units, enhanced situational awareness, fast global command, control, and communications, and improved decision-making. Finally, our framework notes that cyberspace operations can manipulate these effects by either attacking, defending, or sustaining the technological capabilities above.

B. SUMMARY OF FINDINGS

From our thought experiment, we deduced three important findings regarding the use of cyberspace operations on the battlefield. Of note, our findings do not encompass the strategic use of cyber. As we stressed in Chapter I, much analysis has been done regarding the strategic implications of cyberspace operations and the goal of our work is to help turn the debate instead toward its battlefield implications. First, offensive cyberspace operations can broadly be used either to disrupt battlefield systems or to conduct ISR. Both types of operations, if successful, would have significant impacts on battle. Second, synchronization with ground force operations is perhaps the most critical requirement for

disruptive cyberspace operations to have any meaningful battlefield effect. Third, despite the global reach of cyberspace, terrain and enemy still matter regarding what is possible through this new domain.

As is reflected by our theoretical framework, we began this investigation into cyberspace and modern warfare anticipating that battlefield utility would revolve around disruption of technological capabilities. This idea grew out of the ever-increasing connectivity of modern militaries and weapon systems, and the insights of Thomas Rona and others regarding the vulnerabilities of advanced weapons systems. The most surprising insight gained through the thought experiment is that while there are certainly significant opportunities to disrupt battlefield systems through cyberspace operations, using cyberspace operations to conduct ISR could have similarly significant effects on land warfare.

As was represented in our thought experiments, conducting cyber ISR during a conflict could give a belligerent an *enduring* advantage if cyber infiltrations are and remain undiscovered. Foreknowledge of what your enemy will do, when, where, and how they will do it is akin to knowing the future, as was the case with ULTRA in World War II. Having such knowledge almost guarantees achieving surprise on the battlefield or outmaneuvering an opponent. Cyberspace operations that steal data often last months or even years before they are discovered and remediated like ULTRA. Thus, the value gained from one successful offensive cyberspace operation would be multiplied by the battlefield effects achieved over time as a result of having an information advantage.

Contrast the long duration value of gathering operational information with the relatively short duration use of cyber-weapons to disrupt a technological capability on the battlefield. As noted in Chapter III, disruption by its very nature is immediately apparent. While some amount of time may be necessary to identify the cause of the disruption and develop and implement a solution, the immediate battlefield impact of disruption will likely be measured in minutes, hours, or days. While this disruption could prove decisive in battle, military organizations are trained to adapt to contingencies. Therefore, no matter how dependent on any piece of technology, a military organization in combat should quickly adapt to disruption and either fix the problem or operate without the technology.

Nevertheless, even short-term battlefield disruptions can have profound effects on the outcome of a campaign or war.

This finding could be important if a commander has only a limited amount of cyber-weapons. Cyber-weapons are more difficult to employ than traditional munitions. While code can simply be replicated and transported across cyberspace at light speed, cyber-weapons must take advantage of vulnerabilities, whether in hardware, software, or humans, to gain access to their target.[127]

Vulnerabilities must first be discovered, and then an exploit that takes advantage of the vulnerability developed, in order for a cyber-weapon to gain access to a target. While Axelrod and Iliev argue convincingly that there is no shortage of vulnerabilities due to the regular influx of new and updated software coupled with the growing market for exploits, software development and vulnerability patching is a constantly moving target.[128] New versions of common software, such as operating systems, are typically released every few years. Patches for those programs are released much more often, typically weeks or months elapse between patches, and at irregular times based on the severity of the bug or vulnerability being patched.[129] Security researchers and exploit developers are often racing against the clock and each other to find, fix, or exploit vulnerabilities. Clark demonstrated that new software experiences a "honeymoon effect" when it is first released as old tools and exploits are ineffective and attackers are unfamiliar with the code.[130]

Disruptive battlefield cyberspace operations might seem more difficult or less likely, but that assumption might not be correct. We recognize that in conducting only open-source research, our assumptions regarding the difficulty and likelihood of disruptive

---

[127] Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber* Conflict (New York: Kopidion press, 2017), 41, 44.

[128] Robert Axelrod and Rumen Iliev, "Timing of Cyber Conflict," *PNAS,* 1301–1302

[129] Microsoft currently releases security updates monthly and larger feature updates bi-annually. Peter Bright, "Microsoft's Problem Isn't How Often It Updates Windows—It's How It Develops It," Ars Technica, October 20, 2018, https://arstechnica.com/gadgets/2018/10/microsofts-problem-isnt-shipping-windows-updates-its-developing-them/.

[130] Saender Aren Clark, "The Software Vulnerability Ecosystem: Software Development in the Context of Adversarial Behavior" (dissertation, University of Pennsylvania, 2016), 141–42, Publicly Accessible Penn Dissertations.

cyberspace operations against military targets may be overstated. We do not know the extent to which classified capabilities can infiltrate air-gapped networks, disable radar or other hardened sensor systems, or even attack advanced weapon systems themselves such as ballistic missile launchers, tanks, or aircraft. A recent report released by the Government Accountability Office (GAO) concludes that advanced U.S. weapons systems in development are rife with cyber vulnerabilities, which indicates that perhaps disruptive attacks against military systems might be easier and more likely than we imagined in our thought experiment.[131]

With regard to disruptive operations, our thought experiment highlighted the critical role synchronization plays in exploiting the windows of opportunity such disruption creates. If disruption only lasts minutes, hours, or days, then physical battlefield maneuver must be precisely timed and executed within that window.

Such precise synchronization between cyberspace and terrestrial operations is inherently challenging, as noted in JP 3-12(R).[132] Accomplishing the required level of synchronization might require direct command and control of the payload to be employed while also knowing exactly how long it would take to achieve its effects on the target system. Direct command and control are often impossible if the target system is air-gapped. Synchronization may also be achieved through programming a specific date and time for execution of the payload, yet this option could be foiled if the system attacked had incorrect time settings or if the ground forces were unable to achieve the required maneuver at the designated time. Finally, if the payload is incorrectly designed or inadequately tested, it may not function properly, fail to achieve the desired disruptive effects, or cause unintended effects that spread beyond the intended target. These are just a few simple examples, but they seem to align with Libicki's observations on the challenges of synchronization.[133]

---

131 Government Accountability Office, *Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities* (Washington, DC: Government Accountability Office), 2018.

132 Joint Chiefs of Staff, *Cyberspace Operations,* I-8.

133 Libicki, Martin C., *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 99.

Our final finding is that enemy and terrain matter with regard to what battlefield effects are possible through cyberspace. The cyberspace operations conducted by allied forces to enhance situational awareness in Seoul would not be applicable to a tank battle in the desert or SOF teams hunting insurgents in dense jungle. Disrupting satellite communications would be ineffective against an enemy that does not use satellites to communicate. Cyberspace operations require cyberspace along with an enemy or surrounding terrain using machines connected to it. Yet the world is becoming more and more connected; almost every human being on the planet has a cell phone. Cyberspace operations will undoubtedly be considered in all future combat, but what those operations can accomplish on the battlefield will be a direct reflection of the enemy and the terrain.

C. IMPLICATIONS

What do cyberspace operations imply for land warfare? We have three suggestions. First, synchronization should be added to the ever-growing list of principles of warfare. The version of the principles of war elucidated by the Baron Jomini two centuries ago have been a feature of U.S. Army doctrine ever since. These principles have changed little over time; however, current joint doctrine not only renames them the "Principles of Joint Operations," but also includes a handful of new additions to account for military operations across the spectrum of conflict.[134] While our thought experiment does not provide compelling reasons in itself to narrow down the existing list, it does suggest the possible addition of a new principle: synchronization.

The current, largely Jominian, principles are mass, objective, offensive, security, economy of force, maneuver, unity of command, simplicity, surprise, legitimacy, perseverance, and restraint. None of these principles communicate or imply the need for synchronization on the modern battlefield except mass, which we will address shortly. The importance of synchronization in modern warfare predates the recognition of cyberspace as a warfighting domain; it was noted as a significant factor in the United States' success

[134] Joint Chiefs of Staff, *Joint Operations*, JP 3–0 (Washington, DC: Joint Chiefs of Staff, 2017), A-1.

during Operation Desert Storm.[135] The need for, and critical importance of, synchronization in modern warfare is a direct result of the increased speed at which information, forces, and weapons effects traverse the battlefield. The information technologies that underpin cyberspace, as well as all of the capabilities and effects included in our theoretical framework, create major advantages that can only be realized with precise synchronization.

The need for synchronization is reflected in the current joint definition of the principle of mass. It has evolved from one of massed forces at the decisive point to massed effects on the battlefield at the right time and place.[136] This definition not only implies a requirement for synchronization but also provides an argument for replacing mass altogether. The massing of effects by dispersed and disparate forces is contradictory to the actual definition of the word "mass" as a large body of matter. Is victory on the modern battlefield achieved by massing effects at a specific time and place or by precisely choreographing the actions of dispersed forces to achieve a given objective? Special Forces teams synchronized U.S. air power with Northern Alliance ground forces to topple the Taliban in two months in 2001. The synchronization of a coalition joint invasion force toppled the Iraqi government in less than a month in 2003. Boot describes *The New American Way of War* as, "speed, maneuver, flexibility, and surprise…integrate[ing] naval, air, and land power into a seamless whole."[137] Perhaps it is time to abandon the fiction that mass is still a principle of warfare; effects cannot be massed at a place and time without precise synchronization.

Our second suggestion is that a critical element of cyberspace superiority is the ability to quickly recover from attacks on cyberspace capabilities. The idea of cyberspace superiority is not novel. The term is established in JP 3-12(R) and defined as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of

---

135 Arquilla and Ronfeldt, *In Athena's Camp*, 85.

136 Antoine Henri Baron de Jomini, *The Art of War*, Mendell and Craighill translation (Philadelphia, PA: J. B. Lippincott & Co., 1862), 57–58, https://books.google.com/books/about/The_Art_of_War.html?id=nZ4fAAAAMAAJ&printsec=frontcover&source=kp_read_button#v=onepage&q&f=false; Joint Chiefs of Staff, *Joint Operations*, A-2.

137 Max Boot, "The New American Way of War," *Foreign Affairs* 82 (July 2003): 41.

operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary."[138] However, our thought experiment only began to highlight the significant level of dependence that modern armies have on cyberspace. The GAO report referenced earlier notes that virtually every advanced weapon system is connected to cyberspace.[139] Additionally, the requirement for synchronization depends on fast global connectivity; in other words, cyberspace. Many high-technology military capabilities are dependent on space assets, the operation of which depend on cyberspace.[140] For an advanced military like that of the United States' to function properly, it must have cyberspace superiority.

Is superiority in cyberspace even achievable against a peer competitor? As opposed to air or sea superiority, where physical territory can be protected from enemy threats by destroying them as they enter; cyberspace superiority cannot be protected in such a way. Superiority in cyberspace will likely require both the ability to prevent most attacks on the DODIN but also to quickly recover from attacks that are successful. Physical territory will still require physical protection in the other domains, yet even if the joint force is completely successful in protecting the physical infrastructure and the logical network of the DODIN, cyberspace capabilities could still be disrupted through electromagnetic jamming either over broad areas or in precise locations at significant distances. Thus, the ability to quickly adapt to and recover from the compromise, loss, or disruption of a cyberspace capability will be critical to regaining and maintaining cyberspace superiority.

The ability to recover from attacks on cyberspace capabilities covers the entire spectrum of resilience and redundancy to include creating and maintaining data and system backups, having replacement hardware on hand, equipping the force with redundant capabilities, and training the force to react to technological capabilities being disrupted. While the military undoubtedly does all of these things to some extent, codifying the ability to recover as a requirement for achieving and maintaining cyberspace superiority will put

---

138 Joint Chiefs of Staff, *Cyberspace Operations*, GL-4.

139 Government Accountability Office, *Weapon Systems Cybersecurity,* 14.

140 Joint Chiefs of Staff, *Cyberspace Operations*, I-2.

added emphasis on the importance of these tasks and the responsibility for implementing them will be viewed as an operational imperative by the Commander; rather than only a key task of the communications section of the staff.

Finally, cyberspace operations need to be considered as a central part of joint operational planning and execution. The DOD has made many of the organizational changes necessary to implement this with the establishment of USCYBERCOM as a unified combatant command and the U.S. Army's establishment of the cyber branch as a combat arms branch instead of a support branch.[141] However, changes still need to be implemented at the individual and unit level. Operations staffs across the joint force need to understand what cyberspace operations can do and how to integrate them into their larger campaign plan. This requires nurturing individual training and education among the other operations branches as well as growing more cyberspace experts to serve in operational staffs. The U.S. Army is currently working toward building an organic cyber capability into the Brigade Combat Team, and the geographic combatant commands each have aligned cyber mission force teams.[142] These steps are a good start and over time will help build understanding regarding the integration of cyberspace operations with joint operations.

Perhaps this also implies that mission planning, especially mission analysis, needs to adapt. Commanders and staffs plan operations when looking at a map. During mission analysis, the map is populated with overlays and graphics that depict different features of the terrain, enemy, and population to give the operational staff a framework on which to

---

[141] In our opinion, the establishment of USCYBERCOM as a Unified Combatant Command rather than a subordinate command of USSTRATCOM implies a shift in role from a strategic weapon to a maneuver force. Jim Garamone, "Cybercom Now a Combatant Command, Nakasone Replaces Rogers," U.S. Department of Defense, accessed October 24, 2018, https://dod.defense.gov/News/Article/Article/1512994/cybercom-now-a-combatant-command-nakasone-replaces-rogers/; Fort Gordon Public Affairs Office, "Army Cyber Branch Offers Soldiers New Challenges, Opportunities," United States Army, accessed October 24, 2018, https://www.army.mil/article/138883/army_cyber_branch_offers_soldiers_new_challenges_opportunities.

[142] Mark Pomerleau, "Here's How the Army Wants to Integrate Cyber, EW into Operational Formations," Fifth Domain, October 2, 2017, https://www.fifthdomain.com/dod/army/2017/10/02/heres-how-the-army-wants-to-integrate-cyber-ew-into-operational-formations/; "Cyber Mission Force Achieves Full Operational Capability," U.S. Cyber Command, accessed September 20, 2018, http://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/.

build their friendly plan. Because cyberspace cannot be depicted on a traditional map, it is often considered as an afterthought or only a "form of fires" during mission planning. An operational staff will likely view defensive cyberspace operations as a supporting function—simply keeping the communications up and running—while offensive cyberspace operations are likely to be viewed as a form of supporting fires, disabling targets on the physical battlefield.

For cyberspace operations to be understood as a subordinate maneuver capability for the commander, the operations staff needs a visual framework on which to overlay maneuver plans. What should this visual framework look like? Should it be friendly and enemy network maps? Should it be map symbols that indicate potential cyberspace vulnerabilities of specific units or location? Designing a visual framework for planning cyberspace operations that can be set right next to a map of the area of operations would be an interesting follow-up to our research and a step in the right direction in terms of successfully integrating cyberspace operations with military operations in the other domains.

D. A WAY AHEAD: ORGANIZATIONAL PARALLELS TO HUMAN INTELLIGENCE OPERATIONS

We identified several parallels that cyberspace operations share with unconventional warfare and HUMINT operations, especially considering the distinction between Title 10 and Title 50 authorities.[143] These similarities might provide a useful model for assisting operational staffs and commanders in their understanding of cyber as well as organizing those staff sections to better support cyberspace operations. The military's grasp of HUMINT ebbs and flows from commander to commander and we foresee a similar trend developing with cyber. This occurs to the detriment of the capability as it is either underutilized or used incorrectly. Optimizing HUMINT employment requires a commander who understands, and is comfortable with, the tool; we believe the same is true for cyberspace operations.

---

[143] Andru Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3 (2011): 92, http://www.soc.mil/528th/PDFs/Title10Title50.pdf.

Cyberspace operations, like unconventional warfare and HUMINT, require a significant amount of support, long-term planning, and advanced skills. A significant portion of planning for both activities occurs before conflict arises. Military activities prior to a declaration of armed conflict create ambiguity for the application of the means. The often vague delineation of responsibilities between the intelligence and operations sections of a military staff for the employment of HUMINT illustrates the dualistic nature of those activities. Similar confusion could arise when assessing employment of cyberspace operations.

The management of cyberspace operations is most effectively controlled by the operations section, but those operations will at times support information collection requirements from the intelligence section of the staff. The use of HUMINT and unconventional warfare operations as a model for the planning and the management of cyberspace operations by a Joint Staff could help integrate cyberspace operations and terrestrial operations on future battlefields.

E. MERGING BITS WITH BULLETS

Cyberspace is too vital to the proper function of modern militaries for operations within it to be regarded as a support function. In an increasingly interconnected world where every new piece of technology is networked, cyberspace presents countless opportunities—and vulnerabilities—to manifest significant battlefield effects. Thus, either offense or defense can be enhanced or undermined by cyberspace operations. While we broadly classified offensive cyberspace operations as either disruptive or information gathering, when properly integrated into the joint operational plan both can achieve outsized battlefield effects.

To integrate cyberspace operations with joint force operations in the other domains successfully, cyberspace operations need to be understood in terms of the effects they can create on the battlefield. One way to envision these effects is through our proposed cyber-domain interaction framework. Additionally, commanders not only need cyberspace experts as an organic part of their operations and intelligence staff but also a general conceptual understanding of cyberspace operations is needed for all operations officers.

Otherwise, cyberspace operations risk being considered as an afterthought or a supporting function during mission planning rather than as a subordinate maneuver element.

How U.S. military staffs organize for and manage HUMINT operations might be a good model for integrating cyberspace operations as well. The parallels in the need for long-term preparation and highly skilled and specialized individuals indicate there might be benefit in organizing cyberspace operations sections of a joint staff in line with this model. Specifically, creating cyberspace activities subsections as part of both the operations and intelligence sections of the staff to facilitate operational planning and synchronization while also leveraging intelligence assets and fulfilling intelligence requirements.

While we are not challenging the utility or necessity of strategic cyberspace operations, we hope that our study brings attention to, and stimulates the discussion of, what cyberspace operations can mean for land warfare. As long as the discussion continues to focus on the strategic level of war, the U.S. military will continue to struggle to realize the implications that cyberspace has for the battlefield. It will also continue to struggle to integrate cyberspace operations with joint force operations in the other domains. We hope our research has provided a useful contribution to the conversation and a renewed focus on what cyberspace operations mean for combat rather than just what they mean for broader strategic issues in national security and foreign policy.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series. Washington, DC: National Defense University Press, 1999.

Armed Forces Communications and Electronics Association. "The Russo-Georgian War (2008): The Role of the Cyber Attacks in the Conflict," May 24, 2012. https://www.afcea.org/site/defense/cyber-committee.

Arquilla, John. "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers." *Communications of the ACM* 54, no. 10 (October 2011): 58-65.

Arquilla, John, and David Ronfeldt. *Cyberwar Is Coming!* RP-223. Santa Monica, CA: RAND, 1993.

———. *Swarming and the Future of Conflict.* Santa Monica, CA, 2000.

———. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 1997.

Asher, Dani. *The Egyptian Strategy for the Yom Kippur War: An Analysis.* Translated by Moshe Tlamim. London: McFarland and Company, Inc, 2009.

Axelrod, Robert, and Rumen Iliev, "Timing of Cyber Conflict," *PNAS,* 1298-1303, http://www.pnas.org/content/pnas/early/2014/01/08/1322638111.full.pdf.

Barrett, Brian. "The Mysterious Return of Years-Old Chinese Malware." *WIRED*, October 18, 2018. https://www.wired.com/story/mysterious-return-of-years-old-chinese-malware-apt1/.

Bellin, David, and Gary Chapman. *Computers in Battle: Will They Work?* First Edition. Harcourt Brace and Co, 1987.

Berkowitz, Bruce. *The New Face of War: How War Will Be Fought in the 21st Century*. New York, NY: The Free Press, 2003.

BleepingComputer. "Critical RCE Peekaboo Bug in NVR Surveillance System, PoC Available." Accessed September 20, 2018. https://www.bleepingcomputer.com/news/security/critical-rce-peekaboo-bug-in-nvr-surveillance-system-poc-available/.

Boo, Hyeong-wook. "An Assessment of North Korean Cyber Threats," *The Journal of East Asian Affairs* 31, no. 1 (Spring/Summer 2017): 97-117. July 25, 2016. http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf.

Boot, Max, "The New American Way of War," *Foreign Affairs* 82 (July 2003)

Breaking Defense "Artificial Intelligence For Air Force: Cyber & Electronic Warfare." (blog). Accessed August 15, 2018. https://breakingdefense.com/2016/09/artificial-intelligence-for-the-air-force-cyber-electronic-warfare/.

Bright, Peter, "Microsoft's Problem Isn't How Often It Updates Windows—It's How It Develops It," *Ars Technica*, October 20, 2018, https://arstechnica.com/gadgets/2018/10/microsofts-problem-isnt-shipping-windows-updates-its-developing-them/.

Burgess, Matt. "When a Tanker Vanishes, All the Evidence Points to Russia." *WIRED UK*, September 21, 2017. https://www.wired.co.uk/article/black-sea-ship-hacking-russia.

Carter, Ashton. *Department of Defense Cyber Strategy*. Washington, DC: Department of Defense, April 2015.

Cebrowski, Arthur K., and John Garstka. "Network-Centric Warfare: Its Origin and Future." *United States Naval Institute. Proceedings* 124, no 1(January 1998): 28-35, Proquest.

Cha, Frances, and Lucy Corne. "50 Reasons Why Seoul Is World's Greatest City." CNN Travel, July 12, 2017. https://www.cnn.com/travel/article/50-reasons-why-seoul-worlds-greatest-city/index.html.

Chanlett-Avery, Emma, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary. *North Korean Cyber Capabilities: In Brief.* CRS Report No. R44912. Washington, DC: Congressional Research Service, August 3, 2017. https://fas.org/sgp/crs/row/R44912.pdf.

Clark, Saender Aren, "The Software Vulnerability Ecosystem: Software Development in the Context of Adversarial Behavior" (Dissertation, University of Pennsylvania, 2016), Publicly Accessible Penn Dissertations.

Clodfelter, Mark. *The Limits of Air Power*. New York, NY: The Free Press, 1989.

CNBC. "China-Based Hacking Breached Satellite, Defense Companies: Symantec," June 19, 2018. https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html.

Conti, Gregory, and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. New York: Kopidion Press, 2017.

Cordesman, Anthony H., and Charles Ayers. *The Military Balance in the Koreas and Northeast Asia.* Washington, DC: Center for Strategic International Studies, 2016. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161121_korea_book_2016.pdf.

Craig, Murray. "China Missile Launch May Have Tested Part of a New Anti- Satellite Capability." U.S.-China Economic and Security Review Commission Staff Research Backgrounder, May 22, 2013. https://www.uscc.gov/sites/default/files/Research/China%20Missile%20Launch%20May%20Have%20Tested%20Part%20of%20a%20New%20Anti-Satellite%20Capability_05.22.13.pdf.

Defense Acquisition University. "Supportability Strategy for the Transportation Coordinators' Automated Information for Movement System II." Washington, DC: Defense Acquisition University, March 2003, https://www.dau.mil/cop/log/DAU%20Sponsored%20Documents/Supportability%20Strategy%20for%20TC%20AIMS%20II%20DTD%20March%202003.pdf.

Defense Information Systems Agency. "Enabling the Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow." Defense Information Systems Agency, May 2014. https://www.disa.mil/-/media/Files/DISA/About/JIE101_000.pdf.

Defense Information Systems Agency. "JRSS Fact Sheet." Defense Information Systems Agency, April 2017. https://disa.mil/-/media/Files/DISA/Fact-Sheets/JRSS-Fact-Sheet-April-2017.ashx?la=en&hash=68A0F70E92526693C2B824E49068DD52D78091D8.

Defense One. "How to Hack a Military Drone." Accessed June 5, 2018. https://www.defenseone.com/technology/2015/04/how-hack-military-drone/111391/.

Doman, Chris. "The First Cyber Espionage Attacks: How Operation Moonlight Maze Made History." *Medium*, July 7, 2016. https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7.

Eddy, Max. "Satellite Communications Hacks Are Real, and They're Terrifying." *PC Magazine.* Accessed September 21, 2018. https://www.pcmag.com/news/363004/satellite-communications-hacks-are-real-and-theyre-terrify.

Farrell, David N., and Megan Ward. *Megacities and Dense Urban Areas Initiative: Data Collection and Analysis* 16-2955. Washington, DC: MITRE, 2016. https://www.mitre.org/sites/default/files/publications/16-2955-tradoc-g-2-mad-scientists-megacities-analysis.pdf.

FederalNewsRadio. “Operation Gladiator Shield Targeting DOD’s Cyber Terrain.” February 20, 2018. https://federalnewsradio.com/cybersecurity/2018/02/operation-gladiator-shield-targeting-dods-cyber-terrain/.

Fifield, Anna. “A Not-That-Short History of North Korean Assassinations and Attempts,” *Washington Post,* February 15, 2017. https://www.washingtonpost.com/news/worldviews/wp/2017/02/15/a-not-that-short-history-of-north-korean-assassinations-and-attempts/?utm_term=.10b886bc2f51.

Finkle, Jim. “Agent.BTZ Spyware Hit Europe Hard after U.S. Military Attack: Security Firm.” Reuters, March 12, 2014. https://www.reuters.com/article/us-russia-cyberespionage-idUSBREA2B25R20140312.

Fort Gordon Public Affairs Office. “Army Cyber Branch Offers Soldiers New Challenges, Opportunities.” United States Army. Accessed October 24, 2018. https://www.army.mil/article/138883/army_cyber_branch_offers_soldiers_new_challenges_opportunities.Arquilla, John, and David Ronfeldt. *In Athena’s Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 1997.

Fritz, Jason. “Satellite Hacking: A Guide for the Perplexed.” *Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (May 2013): 21-50.

Garamone, Jim. “Cybercom Now a Combatant Command, Nakasone Replaces Rogers.” U.S. Department of Defense. Accessed October 24, 2018, https://dod.defense.gov/News/Article/Article/1512994/cybercom-now-a-combatant-command-nakasone-replaces-rogers/.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (Fall 2013): 41-73.

Gentile, Gian, David E. Johnson, Lisa Saum-Manning, Raphael S. Cohen, Shara Williams, Carrie Lee et al. *Reimagining the Character of Urban Operations for the U.S. Army: How the Past Can Inform the Present and Future*. Santa Monica, CA: RAND, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1602/RAND_RR1602.pdf.

Gordon, Max. “Lessons from the Front: A Case Study of Russian Cyber Warfare.” Research report, Air Command and Staff College, December 2015.

Gould, Joe. “Guided-Bomb Makers Anticipate GPS Jammers.” *Defense News,* August 8, 2017. https://www.defensenews.com/air/2015/05/31/guided-bomb-makers-anticipate-gps-jammers/.

Government Accountability Office. *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities.* Washington, DC: Government Accountability Office, 2018. https://www.gao.gov/assets/700/694913.pdf.

Greenberg, Andy. "How an Entire Nation Became Russia's Test Lab for Cyberwar." *WIRED*. Accessed November 23, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

———. "The Reaper Botnet Has Already Infected a Million Networks." *WIRED*, October 20, 2017. https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

Harris, Marc, Robert Dixon, Nicholas Melin, Daniel Hendrex, Richard Russo, and Michael Bailey. "Megacities and the U.S. Army: Preparing for a Complex and Uncertain Future." Chief of Staff of the Army Strategic Studies Group, June 2014. https://www.army.mil/e2/c/downloads/351235.pdf.

Harrison, Todd, Kaitlyn Johnson, and Thomas Roberts. "Space Threat 2018: North Korea Assessment." Center for Strategic and International Studies, April 11, 2018. https://aerospace.csis.org/space-threat-2018-north-korea/.

Healey, Jason. "Learn Cyber Conflict History or Doom Yourself to Repeat It." *Armed Forces Journal*, December 17, 2013.

Hochfelder, David. "The Telegraph," Essential Civil War Curriculum, Novembe14, 2018. https://www.essentialcivilwarcurriculum.com/the-telegraph.html.

Horner, Charles A. "The Air Campaign." *Military Review* 71, no. 9 (September 1991): 16-27.

ICS-CERT. "Shamoon/DistTrack Malware." Accessed September 14, 2018. https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B.

Irwin, Luke. "How Long Does It Take to Detect a Cyber Attack?" *IT Governance USA* (blog), February 21, 2018. https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/.

Jaitner, Margarita. "Russian Information Warfare: Lessons from Ukraine." In *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: NATO CCD COE Publications, 2015.

Jensen, Benjamin, and David Banks. *Cyberspace Operations in Conflict: Lessons from Analytic Wargames*. Berkeley, CA: Center for Long Term Cybersecurity, April 2018. https://cltc.berkeley.edu/2018/04/16/cyber-operations-conflict-lessons-analytic-wargames/.

Joint Chiefs of Staff. *Cyberspace Operations*. JP 3-12(R). Washington, DC: Joint Chiefs of Staff, 2013.

———. *Joint Communications System.* JP 6-0. Washington, DC: Joint Chiefs of Staff, 2015. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf.

———. *Joint Operations*, JP 3-0. Washington, DC: Joint Chiefs of Staff, 2017.

Jomini, Antoine Henri baron de. *The Art of War*. Mendell and Craighill translation. Philadelphia, PA: J. B. Lippincott & Co., 1862. https://books.google.com/books/about/The_Art_of_War.html?id=nZ4fAAAAMAAJ&printsec=frontcover&source=kp_read_button#v=onepage&q&f=false.

Kaspersky. "Moonlight Maze: Lessons from History." *Kaspersky Labs Daily* (blog). April 3, 2017. https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017.

Koerner, Brendan I. "Inside the OPM Hack, the Cyberattack That Shocked the U.S. Government." *WIRED*, October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution,* November 10, 2017. http://journals.sagepub.com/doi/pdf/10.1177/0022002717737138.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. 1st ed. Washington, DC: National Defense University Press, 2009.

Krause, Peter John Paul. "The Last Good Chance: A Reassessment of U.S. Operations at Tora Bora." *Security Studies* 17, no. 4 (December 9, 2008): 644-84. https://doi.org/10.1080/09636410802508030.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "Brief History of the Internet." *Internet Society* (blog). Accessed June 19, 2018. https://www.internetsociety.org/Internet/history-Internet/brief-history-Internet/.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.

Libicki, Martin C. *What Is Information Warfare?* Washington, DC: National Defense University, 1995.

Lockheed Martin. “Gaining the Advantage: Applying the Cyber Kill Chain Methodology to Network Defense.” 2015. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

Lynch, Justin. “The AI That Protects DOD Networks from Zero-Day Exploits.” Fifth Domain, July 27, 2018. https://www.fifthdomain.com/dod/2018/07/27/the-ai-that-protects-dod-networks-from-zero-day-exploits/.

Mills, Elinor. “USB Devices Spreading Viruses.” CNET, November 20, 2008. http://news.cnet.com/8301-1009_3-10104496-83.html.

Molander, Roger C., Andrew S. Riddile, Peter A. Wilson. *Strategic Information Warfare: A New Face of War*. Santa Monica, CA: Rand, 1996.

Nakashima, Ellen and Missy Ryan. “U.S. Military Has Launched a New Digital War against the Islamic State.” *Washington Post*, July 15, 2016. https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?noredirect=on&utm_term=.195fdff0287a.

National Institute of Standards and Technology. “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.” April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Newman, Lily Hay. “What We Know About Friday’s Massive East Coast Internet Outage.” *WIRED*, October 21, 2016. https://www.wired.com/2016/10/Internet-outage-ddos-dns-dyn/.

Nye Jr., Joseph S. *The Future of Power*. New York, NY: Public Affairs, 2011.

Office of Personnel Management. “OPM Cybersecurity Incidents.” 12 June 2018. https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

Pagliery, Jose. “The Inside Story of the Biggest Hack in History.” CNNMoney, August 5, 2015. https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

Pape, Robert Anthony. *Bombing to Win: Air Power and Coercion in War*. Cornell Studies in Security Affairs. Ithaca, NY: Cornell University Press, 1996.

Paul, Rincon. “Russia Tests ‘Satellite Catcher.’” BBC News, November 20, 2014. https://www.bbc.com/news/science-environment-30097643.

Perlroth, Nicole. “Cyberattack on Saudi Oil Firm Disquiets U.S.” *New York Times*, October 23, 2012, sec. Global Business. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Pomerleau, Mark. “Army Looks to Build Stronger Tactical Cyber Teams.” Fifth Domain, September 14, 2018. https://www.fifthdomain.com/dod/army/2018/09/14/army-looks-to-build-stronger-tactical-cyber-teams/.

———. “Here’s How the Army Wants to Integrate Cyber, EW into Operational Formations.” Fifth Domain, October 2, 2017. https://www.fifthdomain.com/dod/army/2017/10/02/heres-how-the-army-wants-to-integrate-cyber-ew-into-operational-formations/.

Porup, J. M. “It’s Surprisingly Simple to Hack a Satellite.” *Motherboard* (blog), August 21, 2015. https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Rausch, Hank. “Jamming Commercial Satellite Communications during Wartime: An Empirical Study.” Proceedings of the Fourth IEEE International Workshop on Information Assurance 2006 (2006). https://ieeexplore-ieee-org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=1610004.

Raymond, David, Gregory Conti, Tom Cross, and Michael Nowatkowski. “Key Terrain in Cyberspace: Seeking the High Ground.” Tallinn, Estonia: NATO CCD COE Publications, 2014. https://ieeexplore-ieee-org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=6916409.

ReadWrite “Is Seoul the World’s Smartest City?” (blog), May 12, 2016. https://readwrite.com/2016/05/12/is-seoul-the-worlds-smartest-city-ct1/.

Reuters. “Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces.” January 23, 2017. https://www.reuters.com/article/us-saudi-cyber/saudi-telecoms-authority-says-cyber-attacks-have-targeted-websites-idUSKBN1571ZR.

Rona, Thomas P. *Weapon Systems and Information War.* Washington, DC: Office of the Secretary of Defense, 1976.

Secplicity. “What’s Old Is New Again: Why Hackers Reuse Malware.” November 21, 2017. https://www.secplicity.org/2017/11/20/whats-old-new-hackers-reuse-malware/.

Shultz, Richard H. *The Secret War Against Hanoi: Kennedy’s and Johnson’s Use of Spies, Saboteurs, and Covert Warriors in North Vietnam*. First Edition. New York: HarperCollins, 1999.

Smith, Ms. “Saudi Arabia Again Hit with Disk-Wiping Malware Shamoon 2.” CSO Online, January 24, 2017. https://www.csoonline.com/article/3161146/security/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html.

South, Todd. "The Army Is Putting Cyber, Electronic Warfare Teams in Its BCTs." *Army Times,* February 20, 2018. https://www.armytimes.com/news/your-army/2018/02/20/the-army-is-putting-cyber-electronic-warfare-teams-in-its-bcts/.

Standage, Tom. *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's Online Pioneers*. New York, NY: Bloomsbury, 1998.

Sterbenz, James P.G., David Hutchison, Egemen K. Cetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Scholler, and Paul Smith. "Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines." *Computer Networks,* no. 54 (2010): 1245-65.

U.S. Army. *Army Deployment and Redeployment*. ATP 3-35. Washington, DC: Department of the Army, March 2015. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6984_ATP%203-35%20C1%20INCL%20FINAL%20WEB.pdf.

U.S. Army. *Cyberspace and Electronic Warfare Operations* FM 3-12. Washington, DC: Department of the Army, April 2017.

U.S. Army Training and Doctrine Command. "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century." Washington, DC: U.S. Army Training and Doctrine Command, December 2017.

U.S. Cyber Command. "Cyber Mission Force Achieves Full Operational Capability." Accessed September 20, 2018. http://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/.

U.S. Department of Defense. "National Security Space Strategy." January 2011. https://www.defense.gov/News/Special-Reports/National-Security-Space-Strategy/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_/.

Valeriano, Brandon, Benjamin Jensen, and Ryan Maness. *Cyber Strategy: The Changing Character of Cyber Power and Coercion.* New York: Oxford University Press, forthcoming.

Wall, Andru. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal* 3 (2011). http://www.soc.mil/528th/PDFs/Title10Title50.pdf.

White House. "National Security Strategy of the United States of America." December 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

White House. “Remarks by Vice President Pence on the Future of the U.S. Military in Space.” Accessed August 31, 2018. https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-future-u-s-military-space/.

WIRED. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” Accessed May 11, 2018. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California