STRONGPOINT DEFENSE: FROM THE COLD WAR TO CYBERSPACE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JAMES J. TORRENCE, MAJOR, USA
B.S., United States Military Academy, West Point, New York, 2008

Fort Leavenworth, Kansas
2018

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-06-2018	Master's Thesis	AUG 2017 – JUN 2018

4. TITLE AND SUBTITLE

Strongpoint Defense: From the Cold War to Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

James Torrence

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

8. PERFORMING ORG REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
I think the rapid rise of cyber from not being a part of the National Security Strategy to a determinant of U.S. prosperity and security means that policymakers have little or no experience developing cybersecurity strategies. To develop an effective foundation for the creation of cybersecurity strategy, cyber policymakers must learn from Cold War deterrence theory and application. The Cold War dealt with a new type of warfare, rapidly evolving technology, and an environment dominated by the offense which mirrors the current challenges in cyberspace. To build a cyber deterrence strategy, policymakers can look to Cold War deterrence theory to identify principles applicable to defending in cyberspace. The principles of cyber deterrence derived from Cold War analysis are: 1) Cyber deterrence must focus on strongpoints because a perimeter defense will be costly for the defender, and not effective against potential initiators; 2) Critical infrastructure in cyberspace should be encrypted, decentralized, and concealed to increase the cost for the attacker, buy time for the defender, and increase the chance of attribution of the attacker; 3) Researching emerging and future capabilities will create innovation opportunities for long-term cyber defense.

15. SUBJECT TERMS
Strategy, Deterrence, Cyberspace, Cybersecurity, Cold War, Strategic Defense Initiative, Ballistic Missile Defense, Cyberattack, Nuclear, Missiles, Encryption, Concealment, Decentralization

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	154	

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

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major James J. Torrence

Thesis Title: Strongpoint Defense: From the Cold War to Cyberspace

Approved by:

_____, Thesis Committee Chair
Sean N. Kalic, Ph.D.

_____, Member
David W. Mills, Ph.D.

_____, Member
Lieutenant Colonel John E. Turner, MMAS

Accepted this 15th day of June 2018 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

STRONGPOINT DEFENSE: FROM THE COLD WAR TO CYBERSPACE, by Major James J. Torrence, 154 pages.

I think the rapid rise of cyber from not being a part of the National Security Strategy to a determinant of U.S. prosperity and security means that policymakers have little or no experience developing cybersecurity strategies. To develop an effective foundation for the creation of cybersecurity strategy, cyber policymakers must learn from Cold War deterrence theory and application. The Cold War dealt with a new type of warfare, rapidly evolving technology, and an environment dominated by the offense which mirrors the current challenges in cyberspace. To build a cyber deterrence strategy, policymakers can look to Cold War deterrence theory to identify principles applicable to defending in cyberspace. The principles of cyber deterrence derived from Cold War analysis are: 1) Cyber deterrence must focus on strongpoints because a perimeter defense will be costly for the defender, and not effective against potential initiators; 2) Critical infrastructure in cyberspace should be encrypted, decentralized, and concealed to increase the cost for the attacker, buy time for the defender, and increase the chance of attribution of the attacker; 3) Researching emerging and future capabilities will create innovation opportunities for long-term cyber defense.

ACKNOWLEDGMENTS

I want to thank my wife, Nerelyn, for her continued love and support during my time at CGSC. She spent many nights waiting for me to finish my research, so we could have dinner together. I especially want to thank my thesis chair, Dr. Sean Kalic, for his guidance and mentorship throughout this writing process. Dr. Kalic pushed me to be a better writer and thinker which I cannot thank him for enough.

TABLE OF CONTENTS

Page

MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE iii

ABSTRACT iv

ACKNOWLEDGMENTS v

TABLE OF CONTENTS vi

ACRONYMS viii

INTRODUCTION 1

Background 1
Defining Cyberspace 2
National Power Grid Compromise 3
Current United States Cyber Deterrence Situation 4
Deterrence Theory and the Cold War 7
Towards a Cybersecurity Deterrence Strategy 9
Literature Review 10
Background 10
Current Cybersecurity Environment 10
Cybersecurity Deterrence 13
Deterrence Theory 20
Current DoD Deterrence Strategy 24
Conclusion 26

CHAPTER 1 DETERRENCE THEORY 28

Background 28
Defining Deterrence 29
Types of Deterrence Definitions 29
Threat-Based Deterrence 31
Deterrence Not Contingent Upon a Threat 34
Limitations of Deterrence 36
Communication 37
Rationality 38
State-on-State Deterrence Limitations 40
Attribution 43
Arguments for Effective Implementation of Deterrence 45
Unique Deterrence Strategies 45
Defense-Focused Deterrence 47
Deterrence to Provide Options 52

Conclusion 54

CHAPTER 2 DETERRENCE AND MISSILE DEFENSE 56

Background 56
United States Missile Defense 61
Soviet Union Movement Missile Defense 69
Arguments against Missile Defense Systems 74
Conclusion 81

CHAPTER 3 CURRENT CYBER LANDSCAPE AND THE STRATEGIC DEFENSIVE INITIATIVE 83

Background 83
Offensive Advantage in Cyberspace 87
United States Cybersecurity Strategy 92
President Reagan and the Strategic Defense Initiative 96
SDI Guidance 99
Weaknesses of SDI 102
Dividends of SDI 110
Conclusion 113

CONCLUSION LESSONS FOR CYBER POLICYMAKERS 115

Background 115
Defining and Categorizing Cyber Deterrence 116
Encryption 120
Decentralization 124
Concealment 127
Conclusion 132

BIBLIOGRAPHY 134

ACRONYMS

ABM	Anti-Ballistic Missile
BMD	Ballistic Missile Defense
CNA	Center for Naval Analyses
CNAS	Center for a New American Security
CNE	Computer Network Exploitation
CSBA	Center for Strategic and Budgetary Assessments
DSB	Defense Science Board
DARPA	Defense Advanced Research Projects Agency
DCO-RA	Defensive Cyberspace Operations – Response Action
DoD	Department of Defense
DoDIN	Department of Defense Information Network
EMS	Energy Management System
ICBM	Inter-Continental Ballistic Missile
MAD	Mutually Assured Destruction
MIRV	Multiple Independently Targetable Reentry Vehicle
NSDD	National Security Decision Directive
PNNL	Pacific Northwest National Laboratory
RFQ Linac	Radio Frequency Quadruple Linear Accelerator
SAIC	Science Applications International Corporation
SCADA	Supervisory Control and Data Acquisition
SDI	Strategic Defense Initiative
SIFT	Smart Interaction Flow Technologies
SLBM	Submarine-Launched Ballistic Missile

SNF	Strategic Nuclear Forces

INTRODUCTION

Background

> Under such circumstances, retaliation and prevention tend to become indistinguishable, and the distinction between first and second strike becomes blurred. If A has actually originated a first strike against B, then B's nuclear response is a retaliatory second strike. But if A is only suspect, then B's action is a preventive first strike. Since all nuclear powers would have to calculate and operate in this fashion, the proliferation of nuclear weapons implicit in deGaulle's design would result in a political anarchy of unimaginable proportions, followed by total nuclear destruction either piecemeal or in one single catastrophe through the coincidence of a series of preventive-retaliatory blows.
>
> —Hans J. Morgenthau, *The Four Paradoxes of Nuclear Strategy*

Hans J. Morgenthau predicted that increased proliferation of nuclear weapons leads to anarchy because attribution of an attack is not always possible thus resulting in an endless destructive loop with states either retaliating or pre-emptively striking to ensure their security.[1] Morgenthau's theory was never put to the test with a state's use of nuclear weapons, but it foreshadowed the anarchic environment that currently exists in cyberspace. With both state and non-state actors operating in cyberspace, the number of potential perpetrators following a cyber-attack has increased exponentially. The borderless nature of cyberspace coupled with the number of actors makes complete attribution of a cyber-attack nearly impossible. The resulting international situation is the same as the one predicted by Morgenthau. States and non-state actors are engaged in a seemingly endless loop of preventive and retaliatory actions in cyberspace. The type of environment where capabilities are equal and state and non-state actors are in an endless

[1] Hans J. Morgenthau, "The Four Paradoxes of Nuclear Strategy," *The American Political Science Review* 58, no.1 (1964): 35, accessed August 31, 2017, https://www.jstor.org/stable/1952752.

destructive loop makes developing a cybersecurity strategy very difficult. Developing a strategy that deters malicious state and non-state cyber activity against U.S. critical infrastructure is highly complex because of an infinite number of digital vulnerabilities coupled with the problem of attribution.

The United States can develop a cybersecurity strategy with a focus on deterrence in current and future complex operating environments involving numerous actors. Before developing a cybersecurity strategy, a definition of cyberspace is required to ensure those involved with U.S. security operate with a shared understanding. Development of a cybersecurity deterrence strategy for the United States must also account for recent hacks involving critical national infrastructure, existing cybersecurity deterrence strategies, and historical examples of deterrence can inform the development of new ideas.

Defining Cyberspace

Cyberspace is a term that has multiple definitions which creates confusion for those developing cyber strategy. For this paper, the definition of cyberspace used will be from Andrew Krepenivich, who states:

> Cyber space comprises all of the world's computer networks. Thus cyber space includes both open and closed networks and everything they connect and control, to include the computers themselves, the transactional networks that send data regarding financial transactions, and those networks comprising control systems that enable machines to interact with one another, such as Supervisory Control And Data Acquisition (SCADA) systems that regulate pumps, valves, elevators, generators, and other machines[2]

[2] Andrew Krepenivich, *Cyberwarfare: A Nuclear Option?* (Washington, DC: Center for Strategic and Budgetary Assessments), 15, accessed August 27, 2017, http://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option/publication.

Krepenivich's definition of cyberspace is important because it includes open and closed networks, hardware that makes up the internet of things, and SCADA systems which are the present (and likely future) sources of vulnerability to the United States national security interests.

National Power Grid Compromise

On September 6, 2017 hackers "not only compromised energy companies in the US and Europe," but also developed a foothold in the system that afforded them "enough control that they could have induced blackouts on American soil at will."[3] Symantec, the company who found the compromise, did not have enough information to determine the perpetrators of the attack. In fact, they "stopped short of blaming the more recent attacks on any country or even trying to explain the hackers' motives" because they did not have enough evidence.[4] The hackers responsible for gaining a foothold in the United States national power grid had "the ability to stop the flow of electricity into US homes and businesses" and the leading cyber experts in the world do not know who is responsible.[5] The hacker responsible for penetrating the U.S. power grid could be a state actor, a non-state actor operating on behalf of a state actor, or a non-state actor operating as a lone wolf.

---

[3] Andy Greenberg, "Hackers Gain Direct Access to US Power Grid Controls," *Wired,* September 6, 2017, accessed September 29, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

[4] Ibid.

[5] Ibid.

Before the internet "the consequences of power disruption were annoyance and some economic cost" but "now that everything is connected and relies on information provided over a network, the results of a power disruption could be disastrous and range from major power outages to generator explosions (amongst other negative consequences)."[6] Power grids are an example of a SCADA system that is both more efficient and more vulnerable because of the proliferation of networked systems. Increased connectivity makes power grids easier to monitor, more responsive to change, and easier to update remotely. Increased connectivity also makes power grids more susceptible to massive outages because of the interdependence they have on synchronized timing and connectivity with other nodes in their network.

Current United States Cyber Deterrence Situation

The United States power grid was hacked without consequence which is a major national security vulnerability.[7] The power grid is one example of SCADA vulnerability infrastructure susceptible to a cyber-attack. If malicious actors can get into the power grid, they can get into other SCADA systems (i.e., water treatment facilities and controlling gas/oil pipelines). United States cyber strategy is ineffective because it does

[6] Daniel P. Sheperd, Todd E. Humphreys, and Aaron A. Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks" (paper presented at Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Washington, DC, March 19-21, 2012), 2, accessed September 27, 2017, https://radionavlab.ae.utexas.edu/images/stories/files/papers/spoofSMUCIP2012.pdf; James Torrence, "GPS: Infrastructure and Technical Vulnerabilities," *Small Wars Journal,* February 1, 2017, accessed September 1, 2017, http://smallwarsjournal.com/jrnl/art/gps-infrastructure-and-technical-vulnerabilities.

[7] Greenberg, "Hackers Gain Direct Access to US Power Grid Controls."

not deter actors in cyberspace from attacking critical infrastructure (with that said, every country has ineffective cyber deterrence strategies, not just the United States). The Department of Defense (DoD) has not published a cybersecurity strategy since 2015, over which time the processing capability of technology (both enemy and friendly) has doubled.[8] The DoD cyber strategy claims that it "must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests."[9] Admiral Mike Rogers, commander of United States Cyber Command, reinforced DoD's cyber strategy when he asserted one of his organization's top priorities is to "deter or defeat strategic threats to U.S. interests and critical infrastructure."[10] DoD also understands that "vulnerable data systems present state and non-state actors with an enticing opportunity to strike the United States and its interests."[11]

DoD's cyber strategy defines deterrence as working by "convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United

[8] Moore's Law holds that every two years the number of transistors that can fit on a square inch of a circuit card will double and has held true for over 50 years. Moore's Law, though about transistors, is commonly used to describe how computing power and technology capability doubles every two years.

[9] Department of Defense (DoD), *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April, 2015), 10, accessed September 16, 2017, https://www.defense.gov/Portals/1/features/2015/0415_cyber strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[10] Admiral Michael Rogers, *Statement of Admiral Michael S. Rogers Commander United States Cyber Command,* Washington, DC, May 9, 2017, accessed September 29, 2017, https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

[11] DoD, *The Department of Defense Cyber Strategy*, 2.

States, and by decreasing the likelihood that a potential adversary's attack will succeed."[12] DoD's strategy of imposing unacceptable costs on a potential attacker only applies if the United States knows who perpetrated an attack. There is little cost of failure for a state, or non-state adversary, during an attempted cyberattack. Either they complete the attack and walk away unscathed, or they fail and continue to try knowing that the benefits of their success outweigh their minimal chances of getting caught. Conversely, if the United States knows who conducted an attack, then it can effectively use the diplomatic, informational, military, and economic instruments of national power to its advantage. The issue is that it is very rare that the United States will ever be completely sure who conducted (or tried to conduct) a cyber-attack against its national interests. If the United States does not know who conducted an attack, then the only way to convince a potential adversary that it will suffer unacceptable costs if it attacks United States is to develop a cyber defense that will exhaust a malicious actor's time and resources.[13]

Members of the U.S. military and government recognize the shortcomings of current cyber deterrence strategy. The United States, like every country uses ad hoc strategies because there is no historical precedent for the IoT where billions of devices are connected and dependent on one another to operate. Admiral Michael Rogers voiced his concerns about cybersecurity deterrence when he said that "the fundamental concepts

[12] DoD, *The Department of Defense Cyber Strategy*, 2.

[13] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, MD: Rowman and Littlefield, 2017), 166.

of deterrence [in cyberspace] are immature."[14] Senator John McCain "has decried 'the failure to develop a meaningful cyber deterrence strategy'" and many cybersecurity experts "have noted that 'deterrence is an underdeveloped theoretical space in cyber war today.'"[15]

Deterring cyber criminals is critical for the protection of national security interests of the United States. But, the literature and theoretical constructs as to how one should deter criminal cyber activity are still evolving. To develop a foundation from which to build a cyber deterrence strategy, it is first necessary to have a comprehensive understanding of deterrence theory and how deterrence has been used in the past as part of the United States national security strategy.

Deterrence Theory and the Cold War

There are numerous definitions of deterrence, but at its core, deterrence is about convincing someone not to do something. In cyberspace, deterrence is problematic because the United States needs to convince both state and non-state actors that it is not in their best interests to engage in cyber-attacks or cyber espionage against the United States. Deterrence theory rose to prominence during the Twentieth-Century with the advent of nuclear weapons and continues to evolve with more countries creating or acquiring nuclear weapons. Analyzing the evolution of both deterrence theory and Cold

[14] Zachary Goldman and Damon McCoy, "Deterring Financially Motivated Cybercrime," *Journal of National Security Law & Policy* 8, no. 3 (2016): 1, accessed August 28, 2017, http://jnslp.com/wpcontent/uploads/2016/07/Deterring_Financially_Motivated_Cybercrime.pdf.

[15] Ibid.

War deterrence strategy during the Twentieth-Century leads to a general set of deterrence principles that can be applied to cybersecurity deterrence strategy.

Deterrence theorists like Hans Morgenthau. Bernard Brodie, Alexander George, Richard Smoke, Keith Payne, and Steven Quackenbush focused on deterrence relating to state actors using nuclear weapons, so there are inherent limitations in comparing Cold War deterrence to cyber deterrence. But, there are themes that emerged from the Cold War that are directly applicable to cyber security. The theory of "strongpoint defense" outlined by George F. Kennan identified that during the Cold War the United States did not have unlimited resources and should thus concentrate its defense on areas critical to national security.[16] The United States does not have unlimited resources to defend against all possible cyber-attacks which means resources allocated to cyber defense should be concentrated on key infrastructure.

The Cold War also has important parallels to the current cyber environment in that the United States developed a deterrence strategy when it and the Soviet Union each had tens of thousands of nuclear warheads which neither side could defend against. In the current cyber environment, the United States and its adversaries each have cyber capabilities against which there is no defense. The high number of vulnerabilities contrasted with minimal (if any at all) defense capabilities at the height of the Cold War is very similar to the current cybersecurity environment in that offensive capabilities far outweigh defensive capabilities. Deterrence theory has its limitations when applied to the current cyber environment which consists of exponentially more actors and an inability to

[16] John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War* (New York: Oxford University Press, 2005), 27.

identify the perpetrator of an attack. The immaturity of cyber deterrence requires a broader understanding of deterrence theory and strategy to be successfully employed. The Cold War affords one the opportunity to analyze deterrence with two clearly defined states and historical precedent from which one can gain an understanding of deterrence theory and strategy.

Deterrence theorists like Alexander George, Richard Smoke, and Keith Payne agree that effective deterrence theories require unique solutions for each state. Knowing that it is impractical to develop unique strategies for every possible actor in cyberspace, it is necessary to explore how deterrence can be achieved in such a complex operating environment. Analysis of deterrence theory and strategy Twentieth-Century yields general principles required for effective implementation of deterrence as a strategy. General deterrence principles abstracted from theory and historical implementation can be combined with challenges unique to the cybersecurity operating environment to develop a cyber deterrence strategy.

Towards a Cybersecurity Deterrence Strategy

Current attempts at cybersecurity strategy do not discuss how United States' leadership plans to use its power and resources to deter malicious cyber actors from harming United States' national security interests. An effective cybersecurity strategy requires a concept of how leadership will use state power to exercise control of its critical cyber infrastructure to achieve a stronger national security posture.

Chapter 1 outlines the background of Twentieth-Century deterrence theory by analyzing the work of major theorists from the period ranging from definitions of deterrence to strategies for effectively implementing deterrence in national strategy.

Chapter 2 analyzes deterrence strategy used in the Cold War, in particular, the work of George F. Kennan's strongpoint defense applied to anti-ballistic missiles. Chapter 3 analyzes the Strategic Defensive Initiative its application to current cyber deterrence strategy. Chapter 3 concludes with a discussion of lessons identified from Cold War deterrence implementation and how those lessons can be applied to cyberspace. The paper concludes with recommendations for cyber policymakers based on Cold War deterrence theory and application.

Literature Review

Background

Initial research into cybersecurity and deterrence theory resulted in five categories of information: current cybersecurity environment, cybersecurity deterrence, deterrence theory, and current DoD deterrence strategy. This is a qualitative literature review focused on current scholarly work on cybersecurity deterrence and deterrence theory. There is limited existing data on the effectiveness or ineffectiveness of cybersecurity deterrence because it is a relatively new phenomenon. The primary theory being used for this research is deterrence theory.

Current Cybersecurity Environment

To understand the current cybersecurity environment, it is first necessary to define cyberspace, so this literature review operates under a common definition. Almost every author has a different definition of cybersecurity, but the most cited definition of this literature review was the following:

> Cyber space comprises all of the world's computer networks. Thus cyber space includes both open and closed networks and everything they connect and control, to include the computers themselves, the transactional networks that send data

> regarding financial transactions, and those networks comprising control systems that enable machines to interact with one another, such as Supervisory Control And Data Acquisition systems that regulate pumps, valves, elevators, generators, and other machines[17]

This definition of cyberspace is long, but important because it includes SCADA systems which are a major focus of cybersecurity experts. The electric grid is an example of a SCADA system on which cybersecurity scholars have recently focused because of its susceptibility to cyber-attacks from malicious actors.[18] Most scholarly work written in the last five years includes SCADA infrastructure in its cybersecurity discussion which means it should be included in a cyberspace definition.[19]

The largest collection of computer networks resides on the internet. The internet is an ungoverned space "that developed largely outside the control of a single state"[20] which has "challenged the sovereign jurisdictional boundaries of states in ways previously unencountered."[21] The internet is borderless which means any regulation,

---

[17] Krepenivich, *Cyberwarfare: A Nuclear Option?* 15.

[18] Sheperd, Humphreys, and Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks," 2.

[19] Jasper, *Strategic Cyber Deterrence*; Allan A. Friedman and P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014); Jose Romero-Mariona, Megan Kline, and John San Miguel, "C-SEC (Cyber SCADA evaluation capability): Securing critical infrastructures" (paper presented at 2015 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Gaithersburg, MD, November 2-5, 2017), accessed September 29, 2017, http://ieeexplore.ieee.org/abstract/document/7392035/.

[20] Aaron Brantly, "The Most Governed Ungoverned Space: Legal and Policy Constraints on Military Operations in Cyberspace," *Johns Hopkins SAIS Review* 36, no. 2 (2016): 32, accessed September 9, 2017, https://muse.jhu.edu/article/641158.

[21] Ibid.

enforcement, or attribution requires the contribution of other actors on the internet. Borderless inter-related computer networks have also enabled malicious actors (both state and non-state) to conduct criminal activity with little fear of being held accountable. The United States has "turned to international working groups, treaties, and agreements on issues of transnational criminal behavior" because one state simply does not have the resources to prevent criminal behavior on the internet.[22] The current literature focuses heavily on whether the United States can deter malicious cyber actors in the current operating environment. A recently commissioned task force from the Defense Science Board, observed that "although the United States responded with diplomatic moves and economic sanctions to North Korea's Sony hack, China's IP theft, and Russia's meddling in U.S. elections, it is far from clear that such responses have established effective deterrence of future cyber-attacks and costly cyber intrusions."[23]

The Defense Science Board highlighted the major problem discussed in the cyberspace literature: there is little or no evidence that existing attempts at deterring malicious actions in cyberspace have been successful. The lack of success by the United States in deterring malicious cyber actors is complicated when one understands the importance the United States has in projecting cyberspace power on behalf of its allies. The Netherlands Institute of International Relations, Clingendael, released a report in

---

[22] Brantly, "The Most Governed Ungoverned Space: Legal and Policy Constraints on Military Operations in Cyberspace," 32.

[23] Department of Defense (Od), Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017), 3, accessed August 31, 2017, http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

which they argued that "deterring large-scale cyber-attacks is important not only for the United States itself, but also for US allies."[24] The authors of the Clingendael report further observed that United States allies "depend to a considerable degree on the United States to deter large-scale cyber-attacks on themselves."[25]

Cybersecurity deterrence is not only vital to interests of the United States, but also our allies. It is not clear if attempts to deter cyber activity have been effective, or if deterrence of malicious actors in cyberspace is possible. However, further exploration of cybersecurity deterrence may help understand the potential for deterrence in the current cyberspace operating environment.

Cybersecurity Deterrence

Deterrence and cyber deterrence are two terms that have multiple definitions. Understanding the definitions of deterrence and cyber deterrence leads to analysis as to whether any existing definitions are adequate for the development of a cyber deterrence strategy. John Klein argues that "underlying basis of cyber deterrence theory—a subset of general deterrence— is that credible and potentially overwhelming force or other actions against any would-be adversary is sufficient to deter most potential aggressors from

[24] Sico van der Meer and Francil Paul van der Putten. "US Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations," Project Report, September 2015 (project report, Netherlands Institute of International Relations, Clingendael, Netherlands), 2, accessed September 10, 2017, https://www.clingendael.org/publication/danger-proliferating-covert-cyber-operations.

[25] Ibid.

conducting cyberattacks, including those acts considered to be cyberterrorism.[26] The baseline deterrence definition used by scholars is "the process of manipulating an adversary's cost/benefit calculations to prevent him from doing something you do not want him to do."[27] Deterring malicious actors in cyberspace is a Sisyphean task because of the ability of state and non-state actors to initiate cyberattacks from any location in the world.[28] P.W. Singer and Allan Friedman conclude that "without a clear understanding or real reservoir of test cases to study for what works, countries may have to lean more heavily on deterrence by denial" then they did during the nuclear age.[29]

Singer and Friedman show that one of the major problems with cyber deterrence is that countries are working on ad hoc strategies because there are no historical precedents for this type of technology. Admiral Michael Rogers, director of the National Security Agency, echoed the Singer and Friedman's thoughts when he noted that "the fundamental concepts of deterrence [in cyberspace] are immature."[30] Senator John McCain "has decried 'the failure to develop a meaningful cyber deterrence strategy'" and

---

[26] John Klein, "Deterring and Dissuading Cyberterrorism," *Journal of Strategic Security* 8, no. 4 (2015): 29, accessed September 5, 2017, doi: http://dx.doi.org/10.5038/1944-0472.8.4.1460.

[27] Goldman and McCoy, "Deterring Financially Motivated Cybercrime," 1.

[28] Donald Trump, *National Security Strategy of the United States* (Washington, DC: The White House), 12, accessed December 30, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[29] Friedman and Singer, *Cybersecurity and Cyberwar,* 147.

[30] Goldman and McCoy, "Deterring Financially Motivated Cybercrime," 1.

many cybersecurity experts "have noted that 'deterrence is an underdeveloped theoretical space in cyber war today.'"[31]

Deterring cyber criminals is and will continue to play a major part in protecting U.S. national security interests. But, the literature on how one should deter criminal cyber activity is still evolving. Air Force Colonel Timothy McKenzie argues that "it is not possible to deter adversaries from conducting CNE [Computer Network Exploitation] (since the United States will likely be conducting CNE against their systems) but it is possible to deter those activities that cause data corruption, damage, financial loss, or physical injury."[32] The members of the Defense Science Board task force on cyber deterrence further elaborate on the idea that not all cyber-attacks are deterrable. The Defense Science Board cyber deterrence task force contends that "terrorist groups bent on wreaking havoc on the United States" and its allies will most likely not be deterred by the "certain promise of severe punishment."[33] They further argue that, during a major war, "we should not expect to be able to deter even debilitating cyber-attacks on U.S. military capabilities"[34] that do not impact or have minimal damage on civilian society.

The Defense Science Board's task force on cyber deterrence made the argument that cyber- attacks on military capabilities could be separate from public communications

---

[31] Goldman and McCoy, "Deterring Financially Motivated Cybercrime," 1.

[32] Timothy McKenzie, *Is Cyber Deterrence Possible?* (Maxwell AFB, AL: Air University Press, January 2017), 12, accessed August 27, 2017, http://www.au.af.mil/au/aupress/digital/pdf/paper/cpp_0004_mckenzie_cyber_deterrence.pdf.

[33] DoD Defense Science Board, *Task Force on Cyber Deterrence*, 4.

[34] Ibid.

infrastructure, but other scholars argue that "military and civilian networks are often indistinguishable and targeting one could have similar effects on the other."[35] The continued blurring of lines between military and civilian technology creates challenges to existing theories of deterrence that focus specifically on state military capabilities. The overlap between civilian and military operations in cyberspace creates difficulty in the "application of the traditional just war principles of discrimination and proportionality" and has yet to be resolved by existing literature.[36]

Jim Lewis argues that cyber deterrence is not possible because "asymmetric vulnerability to attack, new classes of opponents with very different tolerance of risk, and the difficulty of crafting a proportional and credible threat, all erode the ability to deter in the cyber and space domains.[37] Lewis' major argument is that "the nuclear model of deterrence is not appropriate for the cyber and space domains" because, though the United States has the "most advanced cyber and space forces in the world, these forces fail to deter our opponents from malicious actions" in cyberspace.[38] Lewis does not provide a solution for a new model of cyber deterrence, but he and other scholars make it

[35] C. Anthony Pfaff, "Five Myths about Military Ethics" *Parameters* 46, no. 3 (2016): 66, accessed September 13, 2017, https://ssi.armywarcollege.edu/pubs/parameters/issues/Autumn_2016/9_Pfaff.pdf.

[36] Ibid., 66.

[37] Jim Lewis, "Cyber Deterrence" (Speech presented at Stimson's programming on Space Security, Washington, D.C., 2012), accessed August 26, 2017, https://www.stimson.org/content/jim-lewis-csis-speaks-stimson-cyber-deterrence.

[38] Ibid.

clear that "a state could exhaust personnel and financial resources very quickly trying to exhaust every possible [cyber] threat."[39]

With the understanding that complete deterrence is impractical, the idea of active cyber defense has been introduced as a potential new model for deterrence in the post-nuclear age. The accepted definition of active cyber defense is a set of "offensive actions intended to punish or deter the adversary."[40] Cyber defense consultant Emilio Iasiello argues active cyber defense has two objectives: "1) make adversarial efforts economically or punitively impractical so they stop, and presumably, go on to another target; and 2) cause the decision-making authority to stop directing the hostile activity."[41] Cybersecurity expert Scott Jasper also champions active cyber defense as the most effective cyber security policy to deter malicious cyber actors.[42] Active cyber defense is a reactive system that combines technology with "legal countermeasures beyond network and state territorial boundaries."[43] Active cyber defense is in its initial stages, but requires further analysis to determine its effect as a cyber deterrent against malicious state and non-state actors.

---

[39] Emilio Iasiello, "Hacking Back: Not the Right Solution," *Parameters* 44, no. 3 (2014): 107, accessed September 5, 2017, http://ssi.armywarcollege.edu/pubs/parameters/issues/Autumn_2014/13_IasielloEmilio_Hacking%20Back%20Not%20the%20Right%20Solution.pdf.

[40] Ibid., 105.

[41] Ibid., 108.

[42] Jasper, *Strategic Cyber Deterrence*, 165.

[43] Ibid., 165.

Understanding the cyber deterrence strategies of other state actors assists in the creation of a holistic picture of existing cyber strategies. Russia and China used cyber intrusions as a form of strategic deterrence against the United States. In 2009, the United States "became aware that its electricity network had been hacked" and that the portions of the electricity grid that had been hacked "allegedly could be shut down whenever the hacker wished to do so."[44] Analysis of this cyberattack eventually pointed towards China as the perpetrator with experts asserting that "they [China] left behind software programs that could be used in the future to disrupt" critical infrastructure.[45] China's use of cybersecurity as a foothold for future deterrence (potentially shutting down an electric grid in conjunction with a military maneuver) requires further analysis to understand how the United States can use pro-active defense to deter cyberattacks from malicious state and non-state actors.

Russia also "penetrated U.S. industrial control networks that are responsible for operating critical infrastructure."[46] The Center for Naval Analyses (CNA) posited that "the objective of the hackers appears to have been to develop the capability to remotely access and disrupt control systems in the event of hostilities."[47] The CNA report

---

[44] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (2011): 8, accessed February 10, 2018, doi: http://dx.doi.org/10.5038/1944-0472.4.2.1.

[45] Ibid.

[46] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," (project report, Center for Naval Analyses, Alexandria, VA, March 2017), 28, accessed September 1, 2016, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

[47] Ibid.

concluded with the assertion that "it is possible that the Kremlin is adopting a hold-at-risk approach against U.S. and allied critical civilian infrastructure in order to influence perceived adversaries and deter unwelcome behavior."[48] Like China, Russia used cyber to gain a digital foothold in United States SCADA systems. With this foothold, it is possible to deter future United States action with the threat of manipulating SCADA systems with pre-existing software.[49] The practice of using a digital breach of infrastructure for leverage or deterrence is similar to active cyber defense, but requires further analysis to develop a holistic picture of existing cyber deterrence strategies.

Cyber deterrence is complex. It involves multiple state, and non-state, actors trying to determine the best strategy to deter malicious actors from interfering with their digital infrastructure which has a seemingly infinite number of threat vectors. Jim Lewis, Emilio Iasiello, and C. Anthony Pfaff make it clear that there is a disagreement as to whether cybersecurity deterrence is even possible, and if it is, there is not a consensus as to the best strategy since government and public networks are intertwined.[50] To better understand cyber deterrence, it is necessary to look at the literature of deterrence theory and determine its relevancy to cyber deterrence.

---

[48] Connell and Vogler, "Russia's Approach to Cyber Warfare," 28.

[49] Idaho National Laboratory (Mission Support Center), "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," (project report, Idaho National Laboratory, Idaho Falls, ID, August 2010), ii, accessed February 3, 2018, https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

[50] Lewis, "Cyber Deterrence" (Speech); Iasiello, "Hacking Back: Not the Right Solution, 47; Pfaff, "Five Myths about Military Ethics," 66.

Deterrence Theory

Deterrence theory has its foundations in the writing of Thomas Hobbes, a classical realist thinker. Hobbes discussed deterrence regarding punishment that should be imposed by the state to dissuade man from breaking the law put forth by a sovereign power.[51] Hobbes' major discussion of deterrence posits that "for the punishment foreknown, if not great enough to deterre men from the action, is an invitement to it: because when men compare the benefit of their Injustice, with the harm of their punishment, by necessity of Nature they choose that which appeareth best for themselves."[52] Hobbes' discussion of deterrence was in relation to how the state deters criminals from committing crimes, but his over-arching point is that deterrence is a tool the state wields to dissuade malicious actors through the promise and execution of harsh threats.

Since the writing of Hobbes, deterrence has become a contested theory/concept in international relations. The assumption that a cost/benefit approach will be taken by one's adversary "presupposes rational decision-making processes within the bureaucratic governments of industrially advanced powers" with the expectation industrially advanced powers they will "act according to expected-utility models and cost-benefit calculations."[53] Before the nuclear age, the presupposition of rationality was not considered a major flaw in deterrence theory, but "as thousands of warheads accumulated

[51] Thomas Hobbes, *Leviathan* (New York: Penguin Books, 1968), 339.

[52] Ibid., 339.

[53] James E. Doughtery and Robert L. Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey* (New York: Longman, 2001), 354-355.

in their nuclear arsenals, it became increasingly difficult to believe that rational political leaders could seriously threaten retaliation on a large scale."[54]

Deterrence theory depends on capability and credibility. During the nuclear arms race between the United States and Russia, the increasing number of nuclear weapons made people wonder if the threat of nuclear weapons was still credible. The United States, realizing that it needed a credible threat for effective deterrence, developed a theory of flexible response that afforded them the ability to pose a show of strength using nuclear weapons without using their entire arsenal.[55]

Deterrence theory takes a realist view of the world, which means power is an essential element of deterrence theory. Realists have trouble completely agreeing on a definition of power, but a generally accepted definition of power is "the capacity to produce an intended effect"[56] which Kenneth Waltz adopted and modified from Hobbes.[57] The concept of power has changed in the post-nuclear age with the advent of the internet which led Moises Naim to assert that "a world where players have enough power to block everyone else's initiatives but no one has the power to impose its

[54] Doughtery and Pfaltzgraff, *Contending Theories of International Relations: A Comprehensive Survey*, 354-355.

[55] Ibid., 355.

[56] Kenneth Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 1959), 205.

[57] Ibid.

preferred course of action is a world where decisions are not taken, taken too late, or watered down to the point of ineffectiveness."[58]

Naim's description of a world in which there is a stalemate where state powers block one another's initiatives, and no one can assert power, directly relates to deterrence in the digital age; deterrence is based on having the power (a mixture of capability and credibility) to dissuade someone from doing something. In the digital age, power has changed because the barrier to entry is a computer with an internet connection, not a nuclear weapon. Countries like North Korea "have the capability to make money through cybercrime, from coordinating sophisticated phishing campaigns in buying and selling personally identifiable information, intellectual property and proprietary data, to money laundering in crypto-currencies."[59] Nonstate actors and countries like North Korea can freely attack established powers in the cyber domain because there is limited attribution and no barrier to entry.

The most important point that Naim makes deals with the existence of micropowers. Micropowers are "small, unknown, or once-negligible actors that have found ways to undermine, fence in, or thwart the large megaplayers, the large bureaucratic organizations that once controlled their fields."[60] Micropowers were thought to lack the scale, coordination, resources, and ability to challenge a dominant power. But,

---

[58] Moises Naim, *The End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge Isn't What it Used to Be* (New York: Basic Books, 2013), 18.

[59] Loretta Napoleoni, *North Korea: The Country We Love to Hate* (Australia: UWA Publishing, 2018), 136.

[60] Ibid.

that is no longer the case in the cyber domain where "micropowers are denying established players many options that they used to take for granted. In some cases, the micropowers are even winning contests against the megaplayers."[61]

When looking at deterrence, it is also necessary to understand the neo-realist structural theory put forth by Kenneth Waltz. Waltz, discussing warm, argued that "One cannot say in the abstract that for peace a country must arm, or disarm, or compromise, or stand firm. One can only say that the possible effects of all such policies must be considered" and went onto say that "the peace strategy of any one country must depend on the peace or war strategies of all other countries."[62] Waltz's argument about the peace strategy of one country depending on the peace and war strategies of all other countries, applied to cybersecurity, means that creating a safer cyber domain should consider all policies along with the policies of the other countries operating in the cyber domain.[63]

Waltz's theory of looking at all policies as well as the peace and war strategies of other countries is complicated by the continued advent of new technology. James E. Doughtery and Robert L. Pfaltzgraff recognize that "as military technology becomes more complex, uncertainties in the minds of strategic planners and political decision makers increase" which means "the deployment of each new generation of advanced weapons systems makes it more difficult to calculate the strategic balance and the

[61] Napoleoni, *North Korea: The Country We Love to Hate*, 51-52.

[62] Waltz, *Man, the State, and War,* 222.

[63] Ibid.

possible effects of a nuclear exchange."[64] This passage relates to nuclear weapons, but if one changed the word "nuclear" to "cyber" it would be just as relevant. Understanding policies along with the peace and war strategies of other countries is becoming exponentially more difficult with more advanced cyber weapons and a reliance on electronic systems in both the military and civilian sector.

Deterrence of non-state actors, specifically terrorists, has much broader literature because the presupposition of rationality is not always present with non-state actors. There is a movement in counter-terrorist researcher for deterrence to "be understood from the view of the enemy and their worldview; the deterrence threat must influence them and those who could cooperate with them."[65] The development of a broader perspective on deterring non-state actors requires more research and case-study analysis. The internet has afforded non-state actors the ability to develop cyber weapons that can cause just as much harm as a cyberattack from an established power. Deterring non-state actors will be just as important as deterring state actors for the United States in the future.

Current DoD Deterrence Strategy

The DoD's 2015 cyber strategy remains the most current guiding policy for United States cyber operations. The DoD strategy claims that the United States "must contribute to the development and implementation of a comprehensive cyber deterrence

[64] Doughtery and Pfaltzgraff, *Contending Theories of International Relations*, 355.

[65] Frank Jones, "The Strategic Dimensions of Terrorism: Concepts, Countermeasures, and Conditions in Search for Security," in *Influence warfare: How Terrorist and Governments Fight to Shape Perceptions in a War of Ideas*, ed. J. J. Forest (Westport, CT: Praeger Security International, 2009), 137.

strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests."[66] DoD recognizes that "an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior."[67] DoD's strategy takes into account non-state actors and the important role they play in the cyber domain. DoD's cyber strategy does not provide specific information as to how it will deter non-state actors in cyberspace, though it recognizes how important non-state actors are in the cyber domain.[68]

The DoD realizes that "the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone" but through a myriad of options to include "declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems."[69] The strategy did not address partnerships with civilian organizations (but it did discuss creating and enhancing international partnerships) to share information which was something discussed in other literature for proposals about strengthening network resiliency.

DoD's definition of deterrence was in-line with the ones discussed in this literature review. The Department of Defense claims deterrence "works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the

---

[66] DoD, *The Department of Defense Cyber Strategy*, 10.

[67] Ibid.

[68] Ibid.

[69] Ibid.

United States, and by decreasing the likelihood that a potential adversary's attack will succeed." [70] DoD's strategy also discusses the need for effective response capabilities, resilience of U.S. systems, and a strong information network to ensure that the U.S. can effectively attribute a cyber incident to a state or non-state actor.

Conclusion

Cybersecurity deterrence is an immature strategy conducted ad hoc by states trying to secure their national interests from cyberspace attacks. Development of a cybersecurity deterrence strategy requires a stronger theoretical foundation than currently exists. The 2017 United States National Security Strategy says that America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security."[71] In the 2006 United States National Security Strategy, the word "cyber" was mentioned one time in parentheses.[72] The rapid rise of cyber from not being a part of the National Security Strategy to a determinant of American prosperity and security means that policymakers have little or no experience developing cybersecurity strategies. To develop an effective foundation for the creation of cybersecurity strategy, cyber policymakers must learn from a historical example when destructive weapons, rapidly evolving technology, and an environment dominated by the offense necessitated the United States develop a new defense strategy. The deterrence literature and strategies

[70] DoD, *The Department of Defense Cyber Strategy*, 11.

[71] Trump, *National Security Strategy of the United States*, 12.

[72] George W. Bush, *National Security Strategy of the United States* (Washington, DC: The White House), accessed December 30, 2017, https://www.state.gov/documents/organization/64884.pdf.

created during the Cold War are the best source to develop general principles of deterrence that apply to cyberspace. The Cold War had destructive nuclear weapons, evolving missile and missile defense technology, and an environment that favored the offense. Research on Cold War deterrence theory and Cold War deterrence strategy coupled with analysis that builds parallels to cyberspace will create the foundation from which cyber policymakers can develop an effective cybersecurity deterrence strategy.

CHAPTER 1

DETERRENCE THEORY

Background

> Rational deterrence theory requires not merely internal logical consistency; it must also be operationalized so that the presence of absence of the conditions assumed to be necessary and/or sufficient for deterrence to be effective can be measured and established in each of the specific cases for which predictions are attempted.
>
> —Alexander L. George and Richard Smoke, *Deterrence and Foreign Policy*

Twentieth-Century and Twenty-First-Century deterrence theory focused on nuclear deterrence. Cyber deterrence and nuclear deterrence are not completely analogous but have similar theoretical foundations that require exploration. Analyzing Twentieth-Century and Twenty-First-Century deterrence theory provides insight into how deterrence should be defined, the limitations of deterrence, and general theoretical principles for implementing an effective national security strategy based on deterrence. Deterrence theory was at its height during the Cold War when strategists and scholars tried to determine what type of national security strategy could prevent a nuclear war. Military strategist Herman Kahn best summed up the two questions deterrence theorists tried to answer during the Cold War: "1) How high a quality deterrent does a country need? 2) What kind of strains should the deterrent be able to resist."[73] The canon of deterrence literature produced in such a brief time-period makes it an excellent baseline from which one can abstract general principles of deterrence.

[73] Herman Kahn, *On Thermonuclear War* (Princeton, NJ: Princeton University Press, 1960), 133.

Defining Deterrence

Types of Deterrence Definitions

Analysis of deterrence literature reveals that deterrence does not have a universal definition.[74] Developing a proper definition of deterrence is the foundation on which any further recommendations involving deterrence as a strategy in cyberspace should stand. The danger of not defining deterrence before proposing a new deterrence policy is evident in the work of Keith Payne. Payne wrote *The Fallacies of Cold War Deterrence and a New Direction* in which he never explicitly defined the term "deterrence."[75] Payne claimed that a "healthier understanding of the term [deterrence]" is needed and that his arguments would prove it.[76] But, he still did not explicitly define deterrence.[77] Failure to define deterrence when discussing, critiquing, or proposing deterrence theory is not limited to Payne. Many theorists and political scientists discuss deterrence (some levying

[74] Bernard Brodie, "The Anatomy of Deterrence," *World Politics* 11, no. 1 (1959): 173-191, accessed August 27, 2017, https://www.jstor.org/stable/2009527; Stephen Quackenbush, "Deterrence theory: where do we stand?" *Review of International Studies* 37, no. 2 (2011): 741-762, accessed August 25, 2017, https://www.jstor.org/stable/23024618; Jack S. Levy, "Deterrence and Coercive Diplomacy: The Contributions of Alexander George," *Political Psychology* 29, no. 4 (2008): 537-552, accessed August 25, 2017, https://www.jstor.org/stable/20447143.

[75] Keith Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: The University Press of Kentucky, 2001).

[76] Ibid.

[77] Ibid., 98.

major critiques on deterrence theories of others) without ever providing a definition.[78] A theory without its quintessential term defined leaves open the possibility of ambiguous interpretation. Deterrence is a term that has multiple definitions. Defining deterrence and understanding deterrence theory is the first step towards applying deterrence to cybersecurity.

Understanding the range of deterrence theories is important when identifying lessons that apply to cyberspace. Deterrence theories focus on a cost/benefit analysis conducted by a potential attacker. Deterrence definitions differ regarding the use of threats. Joseph Nye argues that some theorists think deterrence "is inseparable from the threat of retaliatory punishment but deterrence is a concept that has been used with various connotations," not just with the use of a threat.[79] Some deterrence definitions necessitate the use of a threat to achieve a desired outcome, and others think a desired outcome is achievable without necessitating a threat.[80] Analysis of threat-based deterrence theory and deterrence theory not contingent on threats is important for understanding the potential application of deterrence to cyberspace. In a Cold War construct with state actors and nuclear weapons, it is much easier for states to

[78] Alexander George and Richard Smoke's article, "Deterrence and Foreign Policy," *World Politics* 41, no. 2 (1989): 170-182, does not contain a definition of deterrence and required research of their book *Deterrence and American Foreign Policy* to view their deterrence definition.

[79] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 52, accessed September 26, 2017, doi: 10.1162/ISEC_a_00266.

[80] Gary Schaub, Steven Quackenbush, Hans Morgenthau, Paul Huth, and Bruce Russet have threat-based deterrence definitions. Alexander George, Richard Smoke, Joseph Nye, and Bernard Brodie have definitions of deterrence not contingent upon a threat.

communicate threats with other states. In cyberspace, states can still communicate threats to other state actors. But, there is no guarantee that a state can communicate threats to nonstate actors contemplating malicious cyber activity. If a state does not have the ability to communicate a threat to a potential attacker, then a potential malicious actor will not know the threat exists. If a potential attacker does not know a threat exists, threat-based deterrence is ineffective. Developing a cybersecurity deterrence strategy necessitates the understanding of threat-based deterrence when communication with potential actors is possible, and other forms of deterrence applicable to an environment where communication of a threat is not possible.

Threat-Based Deterrence

Bernard Brodie posits that "the threat of war, open or implied, has always been an instrument of diplomacy by which one state deterred another from doing something of a military or political nature which the former did not wish the latter to do."[81] Brodie does not argue that deterrence strategy necessitates a threat, but that threats have always been a method states use to deter military and political action by other states.[82] There is a group of deterrence theorists who believe that a threat, or use of force, is the primary method of

[81] Brodie, "The Anatomy of Deterrence," 174.

[82] Ibid.

achieving deterrence.[83] Gary Schaub argues that "deterrence links a demand that the adversary refrain from undertaking a particular action to a threat or use of force if it does not comply."[84] Stephen Quackenbush echoes Schaub's thoughts by defining deterrence as "the use of a threat (explicit or not) by one party in an attempt to convince another party to maintain the status quo."[85] Quackenbush further elaborates on his definition and argues that "a state must persuade potential attackers that: 1) it has an effective military capability; 2) that it could impose unacceptable costs on an attacker, and 3) the threat would be carried out if attacked."[86] Quackenbush's elaboration on his initial definition of deterrence reveals key tenets of threat-based deterrence: capability and credibility.

Hans Morgenthau expounds on the notion of capability and credibility, when he says that "the appearance of possessing both the ability and the resolution to make good threat and counterthreat becomes, then, of paramount importance as a condition for the success of mutual deterrence."[87] Lawrence Freedman further discusses the importance of capability and credibility and says: "no matter how sincere the deterrer might be in his

---

[83] Gary Schaub Jr., "Deterrence, Compellence, and Prospect Theory*," Political Psychology* 25, no. 3 (2004): 390, accessed August 25, 2017, https://www.jstor.org/stable/3792549; Quackenbush, "Deterrence theory: where do we stand?," 741; Morgenthau, "The Four Paradoxes of Nuclear Strategy," 24; Paul Huth and Bruce Russett, "Testing Deterrence Theory: Rigor Makes a Difference," *World Politics* 42, no. 4 (1990): 469, accessed August 25, 2017, https://www.jstor.org/stable/2010511?seq=1#page_scan_tab_contents.

[84] Schaub Jr., "Deterrence, Compellence, and Prospect Theory," 390.

[85] Quackenbush, "Deterrence theory: where do we stand?" 741.

[86] Ibid., 740.

[87] Morgenthau, "The Four Paradoxes of Nuclear Strategy, 24.

conditional threats, if the opponent does not take these threats seriously then deterrence will fail."[88] Schaub, Quackenbush, Freedman, and Morgenthau primarily focus on military threats in their definitions. Threat-based deterrence does not always contain military threats. States have other instruments of power through which it can make threats to a potential attacker.

Paul Huth and Bruce Russet put forth a definition that includes threats without the use of military action.[89] Paul Huth and Bruce Russet further argue that a:

> rational theory of deterrence focuses on the policies and capabilities a defender can use to persuade an attacker not to initiate some specified action. (For the moment, we will assume the specified action is the use of military force.) The defender has two different kinds of policy instruments to influence the decisions of the attacker: the threat of sanctions and the offer of rewards or inducements.[90]

Huth and Russet's definition does not include the military as a policy instrument of the defender when discussing methods that can be used to influence the decision of the attacker.[91] Huth and Russet's definition of deterrence shows that threats can be any

---

[88] Lawrence Freedman, "General Deterrence and the Balance of Power," *Review of International Studies* 15, no. 3 (1989): 201, accessed August 25, 2017, https://www.jstor.org/stable/20097179.

[89] Schaub Jr., "Deterrence, Compellence, and Prospect Theory," 390; Quackenbush, "Deterrence theory: where do we stand?" 741; Morgenthau, "The Four Paradoxes of Nuclear Strategy, 24.

[90] Huth and Russett, "Testing Deterrence Theory: Rigor Makes a Difference," 469.

[91] Ibid.

instrument of national power a state can wield to dissuade a potential attacker from acting.[92]

Threat-based deterrence requires the defender to communicate threats or use of force to a potential attacker.[93] Threat-based deterrence succeeds when a potential attacker decides the costs of acting outweigh any possible benefits. In cyberspace, states do not always have the capability, or credibility, to have a solely threat-based deterrence strategy. The cyberspace operating environment makes it difficult for a state to communicate a threat to every potential attacker. In a state system, official diplomatic channels exist to communicate messages. No official channels exist for communication in the cyber environment which means a state may never communicate its intent to use a threat to potential attackers. Threat-based deterrence strategies are an option for state actors in cyberspace but are not comprehensive enough to apply to every actor. Deterrence theories not contingent on the communication of a threat to a potential attacker require analysis to determine if they apply to nonstate actors in cyberspace.

Deterrence Not Contingent Upon a Threat

Alexander George and Richard Smoke are two of the leading proponents of a deterrence policy that does not necessarily involve a threat.[94] They claim that "deterrence is simply the persuasion of one's opponent that the costs or risks of a given course of

---

[92] Huth and Russett, "Testing Deterrence Theory: Rigor Makes a Difference," 469.

[93] Freedman, "General Deterrence and the Balance of Power," 200.

[94] Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 182.

action he might take outweigh its benefits."[95] Brodie's definition of deterrence is akin to Smoke and George's. He says the deterrent makes a potential "opponent to consider, in an environment of great uncertainty, the probable cost to him attacking us against the expected gain thereof."[96] Nye also agrees that deterrence does not have to be threat-based and argues that "deterrence is a broader concept than most people think, and that it does not have to rely on military force."[97] Nye defines deterrence as "dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."[98] In Herman Kahn's *On Thermonuclear War*, he discusses nonmilitary deterrents in-depth and argued that "internal reactions or costs" and "losing friends or antagonizing neutrals" are two examples of deterrents not based on threats.[99] Deterrence definitions by Smoke, George, Brodie, and Nye all require analysis by the potential attacker to weigh the potential gains of action against expected risks.[100]

The definitions of deterrence proposed by Morgenthau, Smoke, George, Quackenbush, Schaub, Brodie, Nye, Huth, Russet, and Freedman are the theoretical foundation for understanding how deterrence applies to cyberspace. Threat-based

---

[95] George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice,* 182.

[96] Brodie, "The Anatomy of Deterrence," 179.

[97] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 52.

[98] Ibid.

[99] Kahn, *On Thermonuclear War*, 285.

[100] George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, 182; Nye Jr., "Deterrence and Dissuasion in Cyberspace, 45; Brodie, "The Anatomy of Deterrence," 179.

deterrence theory applies to cyber deterrence of state actors. Threat-based deterrence requires a state communicate its intent to use a threat to dissuade a potential attacker from acting. Every state is a potential attacker in cyberspace. States have official channels of communication. Official channels of communication can be used by a state to communicate a threat to other states thinking about conducting a cyberattack. Deterrence not based on a threat directly applies to nonstate actors in cyberspace. No official channels of communication exist between state and nonstate actors. An inability to communicate threats to a potential attacker means that a state needs other methods of deterrence to ensure an attacker weights the potential gains of an action against the expected risks. Though directly applicable to cyberspace, deterrence still has limitations. The limitations of deterrence as a strategy require analysis before applying deterrence to cyberspace. Cyber policymakers must understand the limitations of a deterrence strategy to ensure they have a realistic understanding of what cyber deterrence will accomplish.

Limitations of Deterrence

Deterrence requires effective communication between the state and the potential challenger.[101] Without effective communication from the state and shared understanding from the challenger, scholars argue that deterrence is likely to fail.[102] Deterrence theory

[101] Freedman, "General Deterrence and the Balance of Power," 201; Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 31.

[102] Ibid.

also makes an inherent assumption that states and potential challengers are rational.[103] An assumption of rationality is problematic because the state assumes a potential challenger will make the most rational decision (rational according to the state) when deciding whether to attack which is not always the case.[104] Deterrence theory is also limited because case studies of state-on-state deterrence strategy do not apply to general deterrence that includes conflicts other than nuclear and actors other than states.[105]

Communication

Lawrence Freedman argues that "the problem with designing deterrence strategies has therefore been to find ways of ensuring that the opponent receives the threat, relates it to his proposed course of action and decides as a result not to go ahead as planned."[106] Freedman further claims that "no matter how sincere the deterrer might be in his conditional threats, if the opponent does not take these threats seriously then deterrence will fail."[107] Freedman's argument is that deterrence is contingent upon communication. A state's ability to use deterrence as a strategy is contingent not upon a state's credibility

[103] Levy, "Deterrence and Coercive Diplomacy", 546; Quackenbush, "Deterrence theory: where do we stand?" 749; George and Smoke, "Deterrence and Foreign Policy," *World Politics* 41, no. 2 (1989): 172, accessed August 25, 2017, https://www.jstor.org/stable/2010406?seq=1#page_scan_tab_contents.

[104] George and Smoke, "Deterrence and Foreign Policy," 172.

[105] Ibid.

[106] Freedman, "Deterrence and the Balance of Power," 201.

[107] Ibid.

and capability, but instead on its ability to successfully communicate a threat to the challenger without the message being lost in translation.[108]

Payne discusses the same challenge of communication in deterrence strategy and says "even the most brilliantly presented deterrence threat may be discounted or misunderstood by the challenger."[109] Freedman and Payne's identification of communication as a major limitation of deterrence strategy focuses on a state-on-state construct. Communication of a cyber deterrence strategy is even more complicated than a state-on-state construct because of the exponential number of challengers to whom a state must communicate. Deterrence not only requires effective communication, but also requires analyzing the assumption that potential attackers will always make the most rational decision when faced with a threat.

Rationality

Payne argues that the assumption that all actors are rational will "greatly challenge Washington's capacity to anticipate a rogue challenger's cost-benefit calculus" and "establish reliable deterrence policies."[110] Jack Levy posits that "deterrence can also fail if the adversary is 'undeterrable,' given its goals and risk-acceptant attitudes."[111] An example of an undeterrable adversary is a suicide bomber. If a potential attacker accepts all risks presented by the defender, regardless of the consequences he faces, he is not

[108] Freedman, "Deterrence and the Balance of Power," 201.

[109] Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 31.

[110] Ibid.

[111] Levy, "Deterrence and Coercive Diplomacy," 546.

deterrable. A determined suicide bomber cannot be successfully deterred no matter how brilliant the deterrence strategy. A suicide bomber's rationality could be questioned by the defender who finds his decision to die during an attack irrational. But, Quackenbush shows the danger in assuming that an actor is irrational. Quackenbush thinks it is obvious that the assumption of actors being rational when developing deterrence theory creates a problem because rationality is subjective and not objective.[112] Quackenbush argues that people are "instrumentally rational" when they make choices according to their preferences, but that "preferences are subjective in nature, emotions, cognitive limitations, and the like may shape preferences but do not make an actor irrational."[113] He goes on to say that "rationality is an inconsistent guide to how deterrence turns out because since: 1) all actions are rational (by assumption) and, 2) deterrence sometimes succeeds and sometimes fails (by observation), this point is obvious."[114] Quackenbush's argument that rationality is subjective further complicates how a deterrence strategy applies to cyberspace. Potential cyberspace attackers have subjective preferences that result in an unpredictable cyber operating environment. An effective cyber deterrence strategy cannot account for the subjective rationality of all potential attackers because it is not practical. Payne, Levy, and Quackenbush show that a general deterrence strategy that assumes the rationality of potential challengers is insufficient because potential challengers may not act in accordance with what the deterring state thinks is rational. The

[112] Quackenbush, "Deterrence theory: where do we stand?" 749.

[113] Ibid.

[114] Ibid.

assumption of rational actors in deterrence theory is based on the state-on-state construct. Deterrence theory, because it is based on Cold War scenarios, is limited by inherent assumptions that deterrence only applies to other state actors.[115]

State-on-State Deterrence Limitations

Smoke and George contend that "deterrence theory at the strategic level, dealing as it does with a relatively simple structural situation, was so much better developed, theorists were tempted to employ the logic of strategic deterrence as a paradigm case for thinking about deterrence in general."[116] Smoke and George realized that that a general deterrence theory based on simple Cold War state relationships would be incomplete because it does not account for a complex environment full of potential state and nonstate attackers. Smoke and George reinforce their argument that state on state deterrence is not sufficient for developing a general theory of deterrence when they claim: "there are (1) the deterrence relationships of the two superpowers' strategic forces; (2) the deterrence of local and limited wars; and (3) the deterrence of nonmilitary challenges and "sublimited" conflict at the lower level of the spectrum of violence."[117] Cyberspace occurs in the "nonmilitary challenges" discussed by Smoke and George.[118] Smoke and George also say that "the interests and motivations (and hence the objectives) of one or both sides are

[115] George and Smoke, "Deterrence and Foreign Policy," 172.

[116] Ibid.

[117] Ibid.

[118] Ibid.

often much more complex and unstable than in simpler, paradigmatic strategic case."[119] When a state tries to deter another state from using nuclear weapons, it knows the physical location of its opponent, understand its opponent's capabilities and potential motivations, and has official channels through which it can communicate a threat or show of strength. In cyberspace, a state does not know the physical location of its opponent, does not understanding its opponent's capabilities or motivations, and has no official channels to communicate.

Any general deterrence theory based on state-on-state case studies is incomplete because it does not account for nonstate actors that occur in operating environments like cyberspace. Keith Payne's theory of deterrence is a perfect example of how a theory developed using state-on-state case studies is incomplete as a theory of general deterrence. Payne's deterrence framework applies to state-on-state deterrence, but does not work as a general theory of deterrence because it does not account for potential nonstate attackers.[120] Payne's deterrence framework "is designed to provide a simple tool for tailoring deterrence policies to specific antagonists and contexts."[121] Payne argues that "pertinent leadership/countries" are one of the "primary areas of interest" for his strategy.[122] Payne's framework aims "to 'get inside' the decision-making process of the challenger, and to ascertain as far as possible the basis for its decision-making with

---

[119] George and Smoke, "Deterrence and Foreign Policy," 172.

[120] Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 102.

[121] Ibid.

[122] Ibid.

regard to a specific context and flashpoint."[123] The end-state of Payne's deterrence framework is to "provide a better basis for anticipating a challenger's behavior."[124] Payne uses many state-on-state case studies to reinforce his proposed deterrence strategy. But, he never discusses deterrence of potential non-state attackers. Payne's deterrence framework operates on the assumption that a state knows its potential attackers and can tailor its strategies to those attackers. Payne's theory is limited, especially with application to cyberspace, because his framework is built on communication between state actors.

Smoke and George warned that the study of strategic deterrence between two states does not constitute enough information to develop general theories of deterrence.[125] Payne's deterrence framework shows the inherent limitations of a general deterrence theory based solely on state-on-state case studies. General deterrence theories based on state-on-state constructs only apply to state relationships in cyberspace. General deterrence theories based on state-on state constructs also assume that a state always knows a potential attacker or the perpetrator of an attack. Attribution in cyberspace is a major problem for general deterrence theory based on state-on-state case studies because it does not have an answer as to how a state should deal with an unknown potential opponent or perpetrator.

---

[123] Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 103.

[124] Ibid.

[125] George and Smoke, "Deterrence and Foreign Policy," 172.

Attribution

Morgenthau recognized the problem of attribution in a multipolar nuclear system.[126] He claimed that "if a multiplicity of nations possessed such devices [nuclear] and the United States had tense relations with only two of them, such an anonymous explosion could with certainty be attributed to no one nation, however much suspicion might point towards a particular one."[127] Morgenthau recognized how difficult it would be for the United States to know who perpetrated a physical attack, even if there were only two potential attackers.[128] Cyberspace attacks occur in the digital realm and have thousands, if not millions of potential attackers. Nye makes the point that "millions of cyberattacks occur every year against all sorts of targets. The Pentagon alone reports more than 10 million efforts at intrusion each day."[129] If determining who committed an attack that involves two potential actors is difficult, determining the perpetrator of an attack with millions of potential actors is nearly impossible. Nye further argued that "knowing the true location of a machine is not the same as knowing the ultimate instigator of an attack."[130] Scott Jasper expands upon the problem of attribution and explains that "states use proxies, groups that act as a substitute for another, to allow for

[126] Morgenthau, "The Four Paradoxes of Nuclear Strategy," 34.

[127] Ibid.

[128] Ibid.

[129] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 47.

[130] Ibid., 50.

'plausible deniability.'"[131] Even if the United States defied the odds and identified both the device and person behind a cyberattack, there is no guarantee that the real motive or other actors involved in the attack will also be identified.

Morgenthau further discussed how "deterrent systems, such as radar and sonar" can identify a physical attack, but not necessarily the country where the attack originated.[132] Morgenthau's description of limited technological capability by the state to identify the perpetrator of a nuclear attack in a multipolar nuclear world mirrors the current cyber situation.[133] The United States government has technical tools to monitor network intrusions and tools to conduct forensics following a cyberattack. Even with these tools, the United States government cannot determine who conducted an attack, or it does not know one of its systems has been breached.[134] Unlike the use of nuclear weapons, cyberattacks are not always evident and can be conducted without the victim ever knowing.

An effective cyber deterrent strategy, especially when attacks can occur without the victim ever knowing, is to deny any potential attacker access to certain cyber infrastructure. Nye asserted that "in the cyber era, deterrence by denial (which is indifferent to attribution)" has regained some of its importance."[135] If a potential attacker

---

[131] Jasper, *Strategic Cyber Deterrence,* 154.

[132] Ibid.

[133] Ibid.

[134] Goldman and McCoy, "Deterring Financially Motivated Cybercrime," 20-21.

[135] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 56.

realizes that it is impractical to breach a certain cyber infrastructure, then he will move on to an easier target. Nye argued that "by chewing up an attacker's resources and time, a potential target disrupts the cost-benefit model that creates an incentive for attack."[136] Attribution is still a major limitation to deterrence strategy. Deterrence by denial, though possible, only applies to certain cyber infrastructure because of finite resources allocated to cyber defense. Deterrence as a national defense strategy does have limitations, but George, Smoke, Payne, and Brodie argue that elements of deterrence can be effectively employed as part of a national security strategy.[137]

Arguments for Effective Implementation of Deterrence

Unique Deterrence Strategies

George, Smoke, and Payne argue that unique deterrence strategies are a prerequisite of effective deterrence.[138] George and Smoke contend that an effective deterrence strategy must "assess the nature and strength of the Initiator's motivation, how urgently he feels the need to challenge deterrence, the options available to him for doing so, the kind of utility calculations and assessment of his options he is likely to be making, and which of them he is likely to choose, if any."[139] Smoke and George argue is that

---

[136] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 56.

[137] George and Smoke, "Deterrence and Foreign Policy," 181; Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 180; Brodie, "The Anatomy of Deterrence," 181.

[138] Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 106; George and Smoke, "Deterrence and Foreign Policy," 180.

[139] George and Smoke, "Deterrence and Foreign Policy," 180.

understanding the initiator "is likely to provide a better understanding of the deterrence problem and what variant of deterrence strategy (alone or together with other policy options) is likely to be appropriate and effective in that particular situation."[140] Smoke and George assert that deterrence strategy is unique to the individual initiator necessitates states conduct unique analysis on all potential initiators to determine the right deterrence strategy.[141] Payne reinforces the arguments of Smoke and George. He introduces a formula for a deterrence policy that requires an understanding of "pertinent leadership/countries, their motivations, goals, and determination, the nature of decision-making, the object of friction (the 'stakes' involved), the regional political/security context, and the sources of power available to the participants."[142]

Smoke, George, and Payne agree that deterrence strategies should be tailored to a potential initiator works in a state construct with finite actors. In cyberspace, developing unique deterrence strategies for every potential actor is not possible. Smoke, George, and Payne's work is focused on deterrence strategies for state actors able to identify potential attackers.[143] The number of potential actors in cyberspace means it is impractical to analyze potential initiators. The limited ability of states to identify the perpetrator of a cyberattack makes the application of Smoke, George, and Payne's work difficult to apply

[140] George and Smoke, "Deterrence and Foreign Policy," 181.

[141] Ibid.

[142] Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 102.

[143] Ibid., 69; George and Smoke, "Deterrence and Foreign Policy," 66.

in cyberspace with the full range of potential actors.[144] Analysis of Smoke, George, and Payne's thoughts on effective deterrence policy reveal that unique state-focused deterrence strategies are not practical in cyberspace as part of a general deterrent.[145] Deterrence "is more difficult in a global environment that is increasingly diverse in its ecology" which makes state-focused deterrence strategies "far more difficult in a changing global system that throws up the unknowable and the unimaginable."[146] State-focused deterrence strategies are not practical for general cyberspace deterrence, but defense-focused deterrence have potential in cyberspace as a general deterrent because they are not state-specific and apply to the full range of potential actors. Bernard Brodie championed a deterrence strategy based on strong defensive measures.[147] Brodie's defense-focused deterrence directly applies to the multipolar cyberspace operating environment.

Defense-Focused Deterrence

Brodie argues for deterrence through the implementation of stronger defense measures.[148] Brodie says that "perhaps the fact that thermonuclear weapons have made it possible, for the first time, to conceive of having more offensive power than we really

---

[144] George and Smoke, "Deterrence and Foreign Policy," 66.

[145] Ibid.

[146] Janice Gross Stein, "Rational Deterrence against Irrational Adversaries," in *Complex Deterrence: Strategy in the Global Age* eds. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago, IL: University of Chicago Press, 2009), 73.

[147] Brodie, "The Anatomy of Deterrence," 181.

[148] Ibid.

need will make it easier to shift emphasis from buying more and better bombers and missiles to buying more and better protection for bombers and missiles."[149] Furthermore, Brodie says "the same kind of problem—deciding how much it is worth paying to design protection into an offensive force—has been faced many times before, notably in the history of warship development."[150] Political Scientist Janice Gross Stein argues that "deterrence becomes fare more difficult when a network has no fixed address, can move easily and hide, and can route its messaging through endangered nodes."[151] Stein's claims that nonstate actors "are more difficult to see, more challenging to manage, and less amenable to the primitive notions of control" previously applied to state power dynamics.[152] Stein's description of the problems of contemporary deterrence portray a complex environment in which policymakers must decide how and where to allocate resources to defend critical infrastructure. Brodie argued that the continued increase of offensive capabilities leads to diminishing returns, which means the focus should shift to enhancing defensive capabilities.[153] Lawrence Freedman also emphasizes the importance of the defense in nuclear deterrence. Freedman says: "the point of deterrence was to persuade a potential adversary not to bank on the first move being decisive, and to think

[149] Brodie, "The Anatomy of Deterrence," 181.

[150] Ibid.

[151] Stein, "Rational Deterrence against Irrational Adversaries," 73.

[152] Ibid.

[153] Brodie, "The Anatomy of Deterrence," 181.

through the consequences of an enemy still capable of fighting back."[154] Though he argues for deterrence by defense, Brodie also realizes that states only have finite resources and that a choice needed to be made as to where to allocate resources for a state's nuclear defense:

> obviously, a much larger proportion of one's total striking force, and preferably the whole of it, has to be given a high level of protection – as well as dispersion and concealment – to make it likely that a reasonable proportion of it will survive. Such a procedure also ensures that the enemy, if he comes at all, has to come with large forces of aircraft, which greatly diminishes his chances for surprise[155]

Further reinforcing the need for selective defense, Brodie says "above all, such a system is not intrinsically capable of being applied to more than a minor portion of one's total force."[156] Professor Mary Manjikian strengthens Brodie's argument about selective defense in cyberspace.[157] Manjikian contends that "deterrence in the cyber-realm is not iterative" and that "deterring one attack does not increase your chances at deterring subsequent attacks."[158] Manjikian further argues that "deterrence is not iterative" which means malicious actors can defeat a static cyber deterrent even if their initial cyberattack

---

[154] Lawrence Freedman, "Beyond Surprise Attack," *Parameters* 47, no. 2 (2017): 10, accessed November 25, 2017, http://ssi.armywarcollege.edu/pubs/Parameters/issues/Summer_2017/4_Freedman_BeyondSurpriseAttack.pdf.

[155] Brodie, "The Anatomy of Deterrence," 181.

[156] Ibid.,

[157] Ibid.

[158] Mary Manjikian, "Deterring Cybertrespass and Securing Cyberspace: Lessons From United States Border Control Strategies," (project report, United States Army War College, Strategic Studies Institute, Carlisle, PA, December 2016), 27, accessed February 13, 2018, https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1332.

fails.[159] Manjikian's argument that cyber deterrents are not iterative is an overly simplistic explanation of a broad range of cyber defenses (some of which are iterative). But, her point about iterative malicious cyberattacks is important for cyber policymakers who must plan and allocate resources for an iterative deterrent to counter a threat that constantly evolves. Applying selective defense espoused by Brodie to critical cyber infrastructure can focus resources on the development of iterative cyber deterrents which can eventually proactively defend against iterative cyberattacks.[160] Brodie understands that a world in which more than one nation had nuclear weapons means that "the potential deterrence value of an admittedly inferior force may be sharply greater than it has ever been before" and that "the kinds of measures in which we ought to be interested are those which could seriously reduce on all sides the chances of achieving complete surprise in a strategic attack."[161]

Brodie recognizes that a multipolar nuclear world created a complex environment where smaller powers could improve their standing with the acquisition or development of nuclear weapons.[162] Brodie's discussion of smaller powers improving their standing directly related to cyber defense where "the amount of malicious actors by nation-states and highly capable actors has increased" which affords more actors the ability to improve

[159] Manjikian, "Deterring Cybertrespass and Securing Cyberspace: Lessons From United States Border Control Strategies."

[160] Brodie, "The Anatomy of Deterrence," 181.

[161] Ibid., 177, 190.

[162] Ibid., 181.

their standing.[163] Brodie predicted that the shift to a defensive focus would be a critical component of a state's deterrent capability because it afforded them the survivability following an attack.[164] Brodie's multiple arguments about the shift to deterrence through defense are directly applicable to cyberspace.[165] Lawrence Freedman also recognized the strength of survivability and said: "first blows are unlikely to be decisive on their own, especially against an opponent with any reserves of strength."[166] Freedman went to far as to say that states should look "to the second and third blows, and also those much further down the line" because states are unlikely to be resilient enough to survive multiple rounds of attacks."[167] The United States depends on SCADA infrastructure to provide services to its citizens and to conduct military operations. Brodie's discussion of deterrence focuses on defending retaliation nuclear capability, but in a cyberattack, there is different infrastructure and capability that requires protection.[168] Brodie focused on defense-based deterrence for a retaliatory strike in a nuclear environment.[169] In a cybersecurity environment that does not involve cataclysmic nuclear weapons, deterrence is beneficial as a strategy to buy more time and afford a defender options when dealing

---

[163] Brodie, "The Anatomy of Deterrence," 181; Nye Jr., "Deterrence and Dissuasion in Cyberspace," 44.

[164] Brodie, "The Anatomy of Deterrence," 182.

[165] Ibid., 181.

[166] Freedman, "Beyond Surprise Attack," 13.

[167] Ibid.

[168] Brodie, "The Anatomy of Deterrence," 182; Freedman, "Beyond Surprise Attack", 13.

[169] Brodie, "The Anatomy of Deterrence," 182.

with a potential attacker. Cyberattacks, though potentially devastating, still occur in a digital realm. Second strike capability may not be the most important part of strong cyber deterrence protecting critical infrastructure. Instead, effective cyber deterrence may provide more time for the defender to identify the potential attacker or narrow down the potential attackers. With more time, the defender can move from a general cybersecurity deterrence strategy to an actor-specific deterrence strategy with a higher likelihood to stop future attacks against critical infrastructure.

Deterrence to Provide Options

Brodie and Freedman argue that deterrence should prevent the initiator from achieving complete surprise. Brodie thinks that strategic warning, "warning of measures being taken that could be a prelude to attack," afforded states the ability to have more retaliatory and defensive options.[170] Brodie's point is that increased strategic warning increased state response flexibility which acted as a deterrence to a potential attacker.[171] Freedman takes it a step further than Brodie and argues that strategic warning must inform "beyond surprise attacks to what follows, to the second and the third blows, and also to those much further down the line."[172] Freedman and Brodie both understand that providing strategic warning to an impending attack can afford a state both more time and more options for a strategic response.[173] Freedman and Brodie's discussion of deterrent

[170] Brodie, "The Anatomy of Deterrence," 182.

[171] Ibid.

[172] Freedman, "Beyond Surprise Attack," 13.

[173] Ibid.; Brodie, "The Anatomy of Deterrence," 182.

as a method of affording states flexibility is a component of deterrence further discussed by Smoke and George.[174] Smoke and George claim:

> Deterrence can severely frustrate an adversary who is strongly motivated to change a status quo that he regards as invidious, especially when he feels it is legitimate to do so. The consequences of continued frustration are not easily predictable and are not always favorable to the deterring power. Deterrence success in the short run is not always beneficial in the longer run; the adversary may become more desperate to mount a challenge and may proceed to acquire greater resources for doing so. Under such circumstances the most reliable benefit of successful deterrence may be more time – time which is best used not in a possible futile effort to maintain deterrence indefinitely but to work out, if possible, an accommodation of conflicting interests as to reduce reliance on deterrence and avoid overt conflict.[175]

Smoke and George argue that the most useful benefit to deterrence may be to buy time.[176] Smoke and George also discuss how good deterrence strategies force potential attackers to find and allocate more resources to continue their attack. Payne, Smoke, and George's discussion of analyzing potential initiators for unique deterrence strategies is not practical for the range of potential actors in cyberspace.[177] But, if a cyber deterrence strategy requires more resources then are available for non-state actors, then it would limit potential initiators to state actors. Nye argues that better cyber defensive measures "enhance deterrence by allowing the government to focus" on more advanced forms of cyberattack.[178] More advanced forms of cyberattack require resources normally

---

[174] Brodie, "The Anatomy of Deterrence," 190; Freedman, "Beyond Surprise Attack," 13; George and Smoke, "Deterrence and Foreign Policy," 182.

[175] Ibid.

[176] George and Smoke, "Deterrence and Foreign Policy," 182.

[177] Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 102; George and Smoke, "Deterrence and Foreign Policy," 182.

[178] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 57.

associated with state actors. With a finite number of potential attackers, unique deterrence strategies become relevant in cyberspace. When defensive measures limit the potential attackers to a finite amount of states with specific resources, unique deterrence measures can be implemented based on models presented by Payne, Smoke, and George. The argument that deterrence can buy a state more time to make decisions made by Smoke, George, and Brodie directly applies to cyberspace. Having more time can lead to attribution, weaken a potential attacker's resolve, and canalize potential attackers into groups that have the capabilities to challenge a resource-intensive deterrent.[179]

Conclusion

Deterrence in cyberspace cannot be threat-based because there is no guarantee a state can communicate its threat to the range of potential actors in the cyber operating environment. Threat-based deterrence is also not effective as a general cyberspace deterrent strategy because of the difficulty of attribution. Deterrence strategy in cyberspace requires measures that do not rely on the communication of threats to potential attackers. A general deterrence strategy in cyberspace needs to "eliminate the majority of potential attacks from unsophisticated users."[180] Deterrence in cyberspace requires a defensive focus on critical cyber infrastructure to limit the number of potential attackers to states. Cyber defensive measures cannot prevent all cyber infrastructure from attack. Limited resources coupled with a massive operating environment necessitate that a state identify and prioritize cyber infrastructure critical to its national security. Once

[179] George and Smoke, "Deterrence and Foreign Policy," 72.

[180] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 57.

identified and prioritized, a state can focus on denying critical infrastructure to potential attackers thereby canalizing them to other potential targets, or mounting a resource-intensive attack on critical infrastructure through other methods (e.g., espionage).

George F. Kennan grappled with the issue of limited resources and prioritization of defensive areas 70 years ago.[181] Analysis of Kennan's strongpoint defense theory along with the evolution of the United States' approach to Cold War deterrence results in applicable lessons to cyberspace. Kennan's strongpoint defense parallels current cybersecurity issues because he understood that it was not practical or possible to defend an entire perimeter against a potential attacker.[182] United States' Cold War strategy evolution shows a continual shift between a focus on offensive measures and defensive measures to find the best method for deterring the Soviet Union from using nuclear weapons.

[181] Gaddis*, Strategies of Containment*, 27, 30.

[182] Ibid.

CHAPTER 2

DETERRENCE AND MISSILE DEFENSE

Background

> Missiles would not be very good at fighting one another. Counter-force attacks by missiles against other missiles were likely to be costly and ineffectual because of the opportunities for protection. Active defense by anti-missile missiles was also liable to be ineffectual because of the speed of the attacking weapons. The only real dual left was between the offense and passive measures for the protection of cities and economic facilities. If it were possible to afford these targets some protection comparable to that being provided for the nuclear forces themselves, then the small warheads of the missile force would have their destruction potential reduced, perhaps to levels acceptable by the defender.
>
> —Lawrence Freedman, *The Evolution of Nuclear Strategy*

In 1948 George F. Kennan "cautioned 'that complete security or perfection of [the] international environment will never be achieved" and that "because capabilities [are] limited, priorities of interest ha[ve] to be established."[183] Kennan argued for "certain categories of needs to which we will be able to respond less promptly and less fully than to others" to ensure "policy of wise economy in the use of our own strength."[184] Kennan evolved his ideas about limited capabilities requiring a prioritization of interests in his theory of "strongpoint defense."[185] Strongpoint defense posits that "concentration on the defense of particular regions and means of access to them, rather than on the defense of fixed lines."[186] Strongpoint defense ran counter to the idea of perimeter defense which

---

[183] Gaddis*, Strategies of Containment*, 27, 30.

[184] Ibid., 30.

[185] Ibid., 57.

[186] Ibid.

"called for resistance to aggression wherever along the periphery" it occurred.[187] Kennan initially championed perimeter defense as a national security strategy to mitigate the Soviet Union's influence in Europe immediately following World War II. But, Kennan shifted to the strategy of strongpoint defense because he realized "no matter how dangerous the external peril, the country had only limited resources with which to fight it" and he did not want to weaken the U.S. strategic economic position.[188] Likewise, Secretary of State George Marshall shifted his thinking to strongpoint defense and claimed that the objective "should be 'to avoid dispersal of our forces when concentration appears to be the wisest cause, especially in view of our present limitations.'"[189] The debate about perimeter versus strongpoint defense that occurred in 1948 applies to Twenty-First-Century cybersecurity. The debate for Twenty-First-Century cybersecurity strategists is how to defend national security interests in cyberspace either through the use of "passive and perimeter-centric defense measures" or through defense measures focused on contested areas "of the defender's internal network."[190] The range of potential attackers capable of remotely harming the United States has exponentially

[187] Gaddis*, Strategies of Containment*, 27, 30.

[188] Ibid.

[189] Ibid.

[190] Center for Cyber and Homeland Security, "Into the Gray Zone: The Private Sector and Active Cyber Defense against Cyber Threats," (project report, Center for Cyber and Homeland Security, Washington, DC, October 2016), 6-7, accessed December 1, 2017, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHActive DefenseReportFINAL.pdf.

increased since 1948 , but the problem of finite resources, multiple targets, and prioritization of protection are common to both situations.

Perimeter defense in cyberspace, like perimeter defense in 1948 around the globe, is not practical or economically responsible. In cyberspace, "if both the attacker and defender are given equal resources, the attacker will prevail" and that a defender trying to "defeat all attacks" will invest more resources than an attacker.[191] In 1948, it was not cost effective or possible for the United States to defend the perimeter of every country susceptible to communist influence or control. Strongpoint defense was important in 1948 because it "allowed the United States to choose the most favorable terrain upon which to confront the Soviet Union."[192] Strongpoint defense also "permitted concentration on areas that were both defensible and vital without worrying too much about the rest."[193] Strongpoint defense operated on the assumption that "not all interests were of equal importance" and that the United States "could tolerate the loss of peripheral areas provided this did not impair its ability to defend those that were vital."[194] Current cyber perimeter defense strategies react to malicious cyber actors in situations that favor the attacker which means perimeter defense is not effective in cyberspace.[195] If the

---

[191] Krepenivich, *Cyber Warfare: A Nuclear Option?,* 84.

[192] Gaddis*, Strategies of Containment*, 58.

[193] Ibid.

[194] Ibid.

[195] Jan van Tol, Mark Gunzinger, Andrew Krepenevich, and Jim Thomas, "AirSea Battle: A Point-of-Departure Operational Concept," (project report, Center for Strategic and Budgetary Assessments, Washington, DC, 2010), 35, accessed November 25, 2017, http://csbaonline.org/research/publications/airsea-battle-concept/publication.

United States chooses a cyber strongpoint defense, then the opportunity exists to canalize the movement of malicious actors in cyberspace and be more proactive in shaping the cyber operating environment.[196] Cybersecurity requires a strongpoint defense to be effective in the deterrence of state actors, as well as nonstate actors. A strongpoint cyber defense must prioritize defensible, vital cyber infrastructure critical to the security of the United States to effectively use finite cyber defense capabilities. Ballistic missile defense during the Cold War is an analogous situation to cyberspace.

The United States and the Soviet Union had finite nuclear missile defense capability, necessitating that each country determine the best allocation of their resources to survive a nuclear attack. Cyberspace also requires the allocation of finite resources to critical infrastructure to ensure survival following a cyberattack. Anti-Ballistic Missile (ABM) implementation during the Cold War is analogous to cyberspace because it represents an attempt by the United States to defend itself from weapons originating from outside of its geographical borders to maintain infrastructure critical to national security (ABMs protected SNF which were critical for deterrence). Analyzing the implementation, success, and failure of strongpoint missile defense during the Cold War provides general principles and lessons identified that apply to the development of a cyber strongpoint defense strategy.

Missile defense during the Cold War is the best comparison to defense in cyberspace. Both the United States and the Soviet Union had multiple nuclear launch sites to include submarines and strategic bombers. The United States and the Soviet Union could not protect all of their Strategic Nuclear Forces (SNF), and therefore had to

[196] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 57.

decide where to allocate their missile defense systems. A perimeter missile defense system was not a realistic option because the United States and the Soviet Union had too many vulnerable locations, including SNF sites and major cities. The only possibility of defending SNFs and population centers was through a strongpoint defense oriented on locations deemed critical to national security.[197] With a strongpoint defense that afforded a state a second-strike capability, deterrence could be achieved. Information technology systems have multiple threat vectors that a perimeter defense cannot effectively address. Perimeter defenses "are fixed targets with relatively static defenses which an enemy can spend time and resources probing for vulnerabilities with little or no threat of retaliation." [198] Perimeter defense in cyberspace can be compared to the Maginot line in that many organizations "spend resources protecting the perimeter of their network with firewalls, intrusion detection systems, and other defensive measures but leave the interior of their networks relatively undefended."[199] Instead of a static perimeter defense, cyber defense must focus on allocating resources to guard infrastructure deemed critical to national security. With critical infrastructure effectively defended, a state can survive a cyberattack and continue to conduct essential operations. The ability to survive a cyberattack through a strongpoint defense can also act as a deterrent to potential attackers. An effective strongpoint cyber defense restricts the pool of potential actors to

---

[197] Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St. Martin's Press, 1981), 136-137.

[198] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," (paper presented at Cyber Conflict (CYCON), 2012 4th International Conference on Cyber Conflict, Estonia, June 5-7, 2012), 10, accessed December 1, 2017, http://ieeexplore.ieee.org/document/6243974/.

[199] Ibid.

those with the time and resources to mount a prolonged cyberattack. Nonstate actors in cyberspace, without partnering with state actors, will not have the resources to effectively defeat a strongpoint cyber defense thus limiting them from attacking infrastructure deemed critical to national security. With the pool of potential attackers limited to states, it is possible to implement state-specific deterrence strategies in conjunction with a strongpoint cyber defense. Missile defense and cyber defense both face the problems of multiple vulnerabilities, finite resources, protection of critical infrastructure, and deterrence through survivability.

Missile defense evolved in both theory and practice during the Cold War. To draw a comparison of defense in cyberspace and missile defense, a chronological discussion of missile defense is not necessary. Instead, an analysis of the themes that ran throughout the evolution of Cold War missile defense theory is a better method for comparing missile defense and cyber defense. Analysis of the strengths and weaknesses of Soviet and U.S. missile defense during the Cold War can provide cyber policymakers with general principles of strongpoint defense that can be applied to defense in cyberspace.

United States Missile Defense

The United States military "readily accepted the importance of the threat of retaliation to deter atomic aggression."[200] General Hap Arnold argued that "[O]ur first line of defense is the ability to retaliate even after receiving the hardest blow the enemy can deliver."[201] Bernard Brodie echoed Gen. Arnold and argued that policymakers should

[200] Freedman, *The Evolution of Nuclear* Strategy, 41.

[201] Ibid.

never lose sight of the "importance of the security of the retaliatory force."[202] To protect its second-strike capability, the United States developed ABMs and ballistic missile defense systems (BMDs). An ABM is "a missile armed with a nuclear warhead, designed to intercept and destroy an incoming missile and prevent it from reaching its target."[203] In 1955, "U.S. national policy called for a strong and effective security posture with emphasis on strategic retaliatory forces and an integrated continental defense system."[204] The United States knew that "such a system [missile defense], truly airtight and in exclusive possession of one of the powers, would effectively nullify the deterrent force of the other, exposing the latter to a first attack against which it could not retaliate."[205] The United States, though it continued to develop offensive nuclear weapons during the Cold War, understood that denying a Soviet nuclear attack could become the ultimate deterrent in the nuclear age.[206]

The development of ABMs and missile defense systems parallels the current problem in cyberspace. National policy-makers want to know how they can implement a

---

[202] Bernard Brodie, *Strategy in the Missile Age* (Princeton, NJ: Princeton University Press, 1959), 285.

[203] Abram Chayes and Jerome B. Wiesner, eds., *ABM: An Evaluation of the Decision to Deploy an Antiballistic Missile System* (New York: Harper & Row, 1969), 4.

[204] Center of Military History, "History of Strategic and Ballistic Missile Defense Volume II 1956-1972," (project report, Center of Military History, Washington, DC, 2009), 1.

[205] Herbert York and Jerome Wiesner, "National Security and the Nuclear Test Ban," *Scientific* American (October 1964), quoted in Freedman, *The Evolution of Nuclear Strategy*, 252-253.

[206] Ibid.

cyber defense strategy that denies a cyberattack by state and nonstate actors against infrastructure critical to United States national security. Understanding the approach towards protecting SNF leads to lessons that directly apply to protecting national security infrastructure in cyberspace. Strategies centered around protecting SNF during the Cold War revolved around the balance between mobility, concealment, and hardened infrastructure.[207] Cyberspace hardened infrastructure is encryption. In cyberspace, data is equivalent to ABMs during the Cold War. The current question surrounding data is how best to protect it from an attack. Like ABMs, data protection requires hardened infrastructure (strong encryption), mobility (decentralization), and concealment (obscuration).

The United States wanted to "detect, identify, and destroy threats to the continental United States as far away as possible."[208] The desire to protect United States SNF from threats required the development of missile defense systems. Shelter was a method of defending ABMs. Kahn argued that:

> Shelter tends to be a good deal more stable than quick reaction alone as a defense, because it is much less accident prone and the number of ways in which it can fail seem relatively low. Unfortunately these few ways can be important. The most worrisome is that if the enemy's attack proves 'larger' than the shelters were built for, the shelters may be negated.[209]

---

[207] Kahn, *On Thermonuclear War*, 263-264.

[208] Center of Military History*, History of Strategic and Ballistic Missile Defense Volume II 1956-1972*, 27.

[209] Kahn, *On Thermonuclear War*, 262.

Kahn recognized that sheltering an ABM was a temporary measure and that shelter was ineffective as the sole measure of defending missile defense systems.[210] Freedman further analyzed the concept of a shelter and reinforced an argument made in *National Policy Implications of Atomic Parity*, a 1958 study by the Naval Warfare Group study, that argued shelters promote a new arms race rather than deter nuclear attacks.[211] The argument from Freedman and the Naval Warfare Group was that shelters to protect nuclear weapons would result in a never-ending loop of stronger weapons built to defeat shelters and then stronger shelters to counter stronger weapons.[212] The Naval Warfare Group study argued that a fortress "challenges the enemy in an arena (endless production of higher-yield, more-accurate missiles) where he is ready and able to respond impressively. Fortress-busting is always possible since any fixed defenses, including all foreseeable anti-ICBM defenses, can be overwhelmed by numbers."[213] Kahn further argued that:

> The attacker may also be able to negate the defender's shelters by exploiting special effects or techniques. For example, he can emphasize ground shock by using weapons that penetrate the earth to explode underground. Unless the equipment is properly shock-protected, it is perfectly possible for the shelter to survive, but for the contents to be useless.[214]

---

[210] Kahn, *On Thermonuclear War*, 262.

[211] Freedman, *The Evolution of Nuclear Strategy*, 167.

[212] Ibid.

[213] The quotation is from an unclassified summary of *National Policy Implications of Atomic Parity* (Naval Warfare Group Study, Number 5, 1958) and a speech by Admiral Burke to the Press Club on 17 January 1958) contained in Freedman, *The Evolution of Nuclear Strategy*, 167.

[214] Kahn, *On Thermonuclear War*, 262.

Kahn and Freedman argued that shelters are ineffective for defense of SNF because they can be overwhelmed by a large enemy attack, they create a new arms race, and they can be exploited through methods other than a direct attack.[215] Cyberspace infrastructure can also be overwhelmed by a large enemy attack, exploited by methods other than a direct attack, and result in arms races for existing vulnerabilities. Encryption alone is not enough to defend data in cyberspace just as shelter alone was not enough to defend SNF during the Cold War. A better solution that included mobility and concealment was needed for SNF just as it is now needed for securing data in cyberspace.

Kahn said: "one way to prevent the attacker from mounting too large an attack is to disperse shelters to many distinct target points. This forces downward the number of missiles the enemy can shoot at each point."[216] Freedman argued that "mobility and concealment" would "discourage an arms race."[217] The 1958 report, *National Policy Implications of Atomic Parity*, also said the "numbers of missiles *National Policy Implications of Atomic Parity* will avail the enemy nothing, if he does not know the location of the target. We in effect take an initiative which he can overcome only by maintaining hour-to-hour fire-comb surveillance of all our land areas and vast oceans [for

[215] Kahn, *On Thermonuclear War*, 262; Freedman, *The Evolution of Nuclear Strategy*, 167.

[216] Kahn, *On Thermonuclear War*, 263.

[217] Ibid.; Freedman, *The Evolution of Nuclear Strategy*, 167.

SNF]."[218] Kahn also championed concealment and mobility. He said "the most exciting kind of protection that is currently being considered is *concealment by continuous mobility or reasonably frequent changes of position.* Now either nobody knows where you are, or it takes extremely up-to-date intelligence for the enemy to be able to follow your movements."[219] Kahn thought that shelter, mobility, and concealment of SNFs would force the enemy to "increase the size of any attacking force."[220]

Brodie agreed with Kahn, Freedman, and the 1958 Navy analysis regarding shelter, mobility, and concealment but he also thought SNF should be dispersed.[221] Brodie argued retaliatory force should be maintained in isolation, dispersed in secret sites, and protected by storage underground.[222] Martin Van Creveld pointed out that the United States changed its methodology regarding SNF from "how to use accurate warheads now available for a 'surgical strike' against the USSR" to determining how to defend SNF against a strike from the Soviet Union.[223] Van Creveld said the United States

---

[218] The quotation is from an unclassified summary of *National Policy Implications of Atomic Parity* (Naval Warfare Group Study, Number 5, 1958) and a speech by Admiral Burke to the Press Club on 17 January 1958) contained in Freedman, *The Evolution of Nuclear Strategy*, 167.

[219] Kahn, *On Thermonuclear War*, 264.

[220] Ibid.

[221] Bernard Brodie*, "*Implications for Military Policy," in The *Absolute Weapon: Atomic Power and World Order,* ed. Bernard Brodie (New York: Harcourt, Brace, and Company, 1946), 76, 88-91.

[222] Ibid.

[223] Martin Van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 9.

"reverse[d] this line of reasoning; they worried about what would happen if the USSR used its MIRVed missiles (the dread SS 18) to 'take out' America's own land-based missiles leaving the United States, if not exactly defenseless, forced to rely on its manned bombers and missile-launching submarines for retaliation."[224] Van Creveld highlighted the courses of action discussed by the United States to maintain the strength of its retaliatory force:

> One was to station American missiles under the sea or else on moving platforms that would crawl over the bottom of the lakes. Another was to lead them on giant trucks and shuffle them from one firing position to the next along an underground 'racetrack' half as large as the American Midwest. A third school proposed digging holes thousands of feet deep. The holes would be sealed, and the missiles inside them provided with special equipment that would enable them to screw their way up to the surface in the aftermath of an attack.[225]

Freedman, Kahn, Brodie, Van Creveld and the Naval Warfare Group identified the problems of shelter, mobility, and concealment of land-based missile defense systems. The increased dispersion, concealment, and shelter of ABM systems necessitated that the enemy exert more resources to find the location of missile defense systems.[226]

Kahn argued that an increase in size of the enemy attacking force would "increase the probability that we will get the warning" of an enemy attack.[227] Kahn recognized that, when the enemy does not know the location of ABMs, he will be forced to widen his

---

[224] Van Creveld, *The Transformation of War,* 9.

[225] Ibid.

[226] Freedman, *The Evolution of Nuclear Strategy*, 167; Herman Kahn, *On Thermonuclear War*, 264.

[227] Kahn, *On Thermonuclear War*, 264.

search, thus requiring more resources.[228] Kennan discussed how strongpoint defense "allowed the United States to choose the most favorable terrain upon which to confront the Soviet Union."[229] Kahn reinforces Kennan's point. If the sheltering, mobility, and concealment of United States ABM systems create early warning for the United States, then the United States proactively shapes its nuclear operating environment to engage enemy nuclear weapons on more favorable terms. A cyber defense strategy should also proactively shape the operating environment to engage malicious actors in a more favorable situation.

Kahn, Kennan, Brodie, Van Creveld, Freedman, and the Naval Warfare Group all discussed issues associated with land-based ABM systems that directly apply to cyberspace. If malicious cyber actors do not know the location of the data for which they are searching, they will be forced to expend time and resources to find that data. Through the expenditure of time and resources, there is a greater chance that the United States will become aware of their efforts, and thus have a greater chance of interdicting before a cyber event occurs. Cyberspace is also unique in that the time and effort required to find data that is sheltered, concealed, and mobile will separate state and nonstate actors because of the resources required.

Denying nuclear missiles is not easy and denying a large barrage of incoming missiles is nearly impossible. Deterrence by denial stops malicious actors from attacking infrastructure critical to national security. During the Cold War, the United States was not

---

[228] Kahn, *On Thermonuclear War*, 264.

[229] Gaddis, *Strategies of Containment*, 58.

the only nation thinking about strategic missile defense. The Soviet Union also developed ABM systems and methodology to deploy BMD systems.

Soviet Union Movement Missile Defense

Soviet Union recognized the merits of a strong defense in the nuclear environment. In 1967, Chairman of the USSR Council of Ministers Alexei N. Kosygin said:

> I think that defensive systems that preempt assault are not the cause of the arms race. They represent a means of preventing death of people. Some post a question: what is cheaper – to have attack weapons capable of annihilating towns and entire states or to have defensive weapons which may prevent such annihilation?... Perhaps, a missile defense system costs more than an attack system but it is aimed not at killing people but saving human lives.[230]

The Soviet Union began working on missile defense systems as early as 1945 when "Georgii M. Mozharovsky initiated the first study of possible defenses against missiles."[231]The Soviet Union anticipated the development of the ICBM and knew it needed to defend itself. In 1953, "perhaps the most important event that ultimately led to a large-scale national missile defense program" occurred when "Chief of the General Staff of the Soviet Army Marshal Vasilii D. Sokolovsky sent a letter to the Central Committee of the Community Party of the Soviet Union" discussing the importance of missile defense.[232] The letter said "it is expected that the probable adversary will have in near future long-range ballistic missiles as the main means of delivery of nuclear charges

---

[230] Mike Gruntman, *Intercept 1961: The Birth of Soviet Missile Defense* (Reston, VA: American Institute of Aeronautics and Astronautics, 2015), 5.

[231] Ibid., 91.

[232] Ibid., 94.

to strategic objects in our country. Air Defense systems, currently deployed and under development, cannot defend against ballistic missiles"[233] In the broader strategic context, the 1962 book, *Soviet Military Strategy*, by Sokolovsky elaborated on USSR's missile defense methodology:

> Protection of the country's rear areas and formations of armed forces from nuclear strikes by the enemy has, as its aims, to preserve the vital activity of the state, to secure the uninterrupted functioning of the economy and transportation, and to safeguard the combat potential of the Armed Forces. These aims will be achieved primarily by destroying the enemy's nuclear weapons where they are based. However, there is no guarantee that significant aircraft and missile forces can be destroyed at their bases, especially at the outset of a war, if the enemy attacks by surprise. Therefore the necessary forces and weapons must be available to destroy large numbers of enemy aircraft and missiles in flight in order to prevent nuclear strikes against the country's most important targets. This can be done by conducting military operations to defend the country from enemy air and missile attack.[234]

Sokolovsky implied that if the Soviet strategic offensive forces were to destroy all potential attackers, defensive forces would be unnecessary.[235] Furthermore, Sokolovsky recognized that it was improbable that a USSR first strike would render the United States incapable of offensive operations which necessitated the development of strategic nuclear defense.[236] Sokolovsky's strategy aimed to destroy SNF at their point of origin with the understanding that a strong defense is required if SNF are not stopped early enough in the

---

[233] Gruntman, *Intercept 1961: The Birth of Soviet Missile Defense,* 94.

[234] Vasilii D. Sokolovsky, *Soviet Military Strategy* (1962 in Russian), accessed February 17, 2018, https://www.rand.org/content/dam/rand/pubs/reports/2005/R416.pdf, 417.

[235] Ibid.

[236] Ibid.

launch process.[237] Sokolovsky also discussed preventing "nuclear strikes against the country's most important targets" which goes back to the Russian implementation of point defense due to finite resources.[238] Sokolovsky's work directly applies to defense in cyberspace.

In cyberspace, the best course of action would be to negate an attack at the point of origin before it ever extends beyond a malicious actor's device. Negating attacks before they occur is technically possible in cyberspace, but not feasible for the range of potential actors, many of whom may conduct surprise attacks. Because not all cyberattacks can be stopped at their point of origin, defensive measures must be established to protect infrastructure critical to national security in cyberspace. Combining Sokolovsky's methodology with the concepts of concealment, mobility, and dispersion create the baseline of cyber defense strategic thinking.

The Soviet Union generally accepted the "concept of zonal or area defense," but the "limited capabilities of available weapons systems and the dispersion of many targets to be defended dictated that in practice a point defense would still be frequently employed."[239] Like the United States, the Soviet Union preferred a perimeter defensive system against nuclear weapons, but limitations in weapons capabilities and resources necessitated they adopt a point or strongpoint defense instead.[240] The Soviet Union's

---

[237] Sokolovsky, *Soviet Military Strategy,* 417.

[238] Ibid.

[239] Center of Military History, *History of Strategic and Ballistic Missile Defense Volume II 1956-1972*, 104.

[240] Ibid.

decision to commit massive "resources to strategic defense also signified the acceptance of the idea that defense was useful and that the possession of a deterrent offensive capability alone would not be enough."[241] Cyberspace offensive weapons are not enough to deter malicious actors. The ubiquity of networked systems coupled with the number of potential malicious actors means that defense, not offense is the key to deterrence in cyberspace. The "volume of malicious code, known as malware, that threatens the functioning of critical infrastructure" has "increased to over 390,000 programs each day."[242] The range of malicious programs coupled with the number of potential state and nonstate actors means that defense, not offense will be the best method of deterring malicious actors in cyberspace.

The Soviet Union's strategy for strategic missile defense "derived from a threat perception which had six main elements:"[243]

> 1. The growing and adapting threat, especially from U.S. strategic offensive forces, necessitates continuing vigilance and a strong commitment of forces to strategic defense.
>
> 2. The multidirectional nature of the threat necessitated an all-around point and area defense, especially in view of the ease with which any kind of barrier defense could be penetrated.
>
> 3. The omnipresent air-breathing bomber threat was real and close at hand and had to be dealt with.

---

[241] Center of Military History, *History of Strategic and Ballistic Missile Defense Volume II 1956-1972*, 104.

[242] Jasper*, Strategic Cyber Defense*, 5.

[243] Center of Military History, *History of Strategic and Ballistic Missile Defense Volume II 1956-1972*, 108.

> 4. The United States was constantly pushing the state of the art in new technology which meant that the appropriate countering technology had to be obtained somehow and had to be adopted and deployed quickly.
>
> 5. The missile threat could not be handled effectively with the capabilities of the National Air Defense Forces; therefore, it was necessary to target MR/IRBMs, and strategic bombers and then ICBMs against the missile launching sites.
>
> 6. Targeting the U.S. means of strategic attack still did not guarantee defense against the missile threat and therefore necessitated acquiescence in strategic arms limitation talks.[244]

The six elements of the USSR's strategic missile defense are very similar to United States methodology towards missile defense. The Soviet Union wanted to counter the U.S. offensive capabilities by employing a strong defense, dispersing their SNFs, avoiding employment of obsolete technology, allocating finite resources to defend key infrastructure, and using defensive deterrence to buy time.[245] The first, second, and fourth element of Soviet strategic missile defense could almost be used word-for-word in a cyber defense strategy. Cyberspace requires strategic defense to keep up with the growing and adapting threat. The multidirectional nature of the cyber threat necessitates avoiding a barrier defense and conducting a point and area (not perimeter) defense. The rapid evolution of technology requires rapid development and implementation loops for defenders to keep up with potential malicious actors. The United States and the Soviet Union both concentrated resources on strategic missile defense during the Cold War. Missile defense systems, though developed, had substantial counter-arguments centered around their actual effectiveness.

---

[244] Center of Military History, *History of Strategic and Ballistic Missile Defense Volume II 1956-1972*, 108.

[245] Ibid.

Arguments against Missile Defense Systems

Missile defense systems in the West had many critics, with the main counter-arguments to BMDs being that they were obsolete when implemented, not completely testable, destabilizing, and ineffective.[246] One argument against missile defense was that the technology proposed at the beginning of a missile project was obsolete during implementation. Freedman noted that "during the 1950s a defensive anti-aircraft system was developed in the United States" which was cutting edge technology during its inception.[247] Though initially advanced technology, Freedman points out that "by the time the [anti-aircraft] system had been developed, it had been rendered obsolete by the imminent arrival of [Intercontinental Ballistic Missiles] ICBMs."[248] Senator John C. Stennis (D-Mississippi) represented the views of policy-makers in opposition to developing missile defense systems when he said: "we are pouring these many hundreds of millions of dollars into ground-to-air defenses, some of which it seems to me is already obsolete."[249]

The technology problem that affected missile defense systems is not analogous to cyberspace. When a missile defense system was rendered obsolete, it required new

---

[246] U.S. Congress, *Hearings before Subcommittee of Committee on Armed Services*, Washington, DC, 1960; Leonard S. Rodberg, "ABM Reliability" in *ABM: An Evaluation of the Decision to Deploy an Antiballistic Missile System*, eds. Abram Chayes and Jerome B. Wiesner (New York: Harper & Row, 1969), 107; George F. Kennan, *Russia, the Atom, and the West* (New York, Harper & Brothers, 1958), 54.

[247] Freedman, *The Evolution of Nuclear Strategy*, 165.

[248] Ibid.

[249] U.S. Congress, *Hearings before Subcommittee of Committee on Armed Services*, 1960.

research, funding, and development to rectify the problem. Developing new missile defense systems takes years. Cyber systems often have software vulnerabilities that enemies exploit to conduct cyberespionage. Unlike vulnerabilities in nuclear defense systems, software vulnerabilities can be rectified in seconds and go into effect when those effected are connected to the internet. The cost of a software upgrade is negligible (if nonexistent) when compared to development of a missile defense system. The speed at which cyber systems can update and defend against enemy intrusion following the identification of a vulnerability is exponentially faster than a missile defense system. Cyber systems are also fully testable when implemented.

Physicist Leonard S. Rodberg[250] argued that "once an ABM system was actually installed, it could never be realistically tested – for an obvious reason."[251] The inability to conduct a full-scale test of ABM systems resulted in false confidence among policymakers. Rodberg argued that "there is a substantial likelihood that, in the course of a complicated engagement involving incoming warheads, decoys, chaff, electronic countermeasures, blackout explosions, and other unpredictable effects, the system would fail completely."[252] Rodberg was skeptical of a missile defense system's ability to perform in perfect conditions, and made a compelling argument that, in realistic conditions, it would most certainly fail.[253] Cyber defense systems do not have the same

[250] Rodberg was also the Chief of Policy, Research, Science, and Technology Bureau, U.S. Arms Control and Disarmament Agency, 1963-1968.

[251] Rodberg, "ABM Reliability," 107.

[252] Ibid., 117.

[253] Ibid.

shortcoming as missile defense systems. Because they do not require the detonation of a nuclear warhead, cyber defense systems are easier to test, iterate, upgrade, and optimize before implementing. The ability to test defense prototypes against malicious activity makes the lessons identified from ABM successes and failures applicable. Even the theory behind ABM development applies to the development of cyber defense systems. The difference being that cyber systems can be tested against the worst known forms of attack before being deployed. George F. Kennan in 1958, and Jerome B. Wiesner and Herbert F. York in 1964, further argued that missile defense systems were destabilizing to U.S. and Soviet Relations.[254] Focus on stability between the United States and Russia eventually resulted in the adoption of Mutually Assured Destruction (MAD) as a strategic policy which "deliberately eschews serious efforts at defense against attack from the air and relies completely on the terror of retaliation to prevent war, leaving no means for defense if deterrence fails."[255]

Assured destruction was the "very essence of the whole deterrence concept" adopted by Secretary of Defense Robert McNamara.[256] McNamara argued that the United States "must possess an actual assured-destruction capability, and that capability must

---

[254] Freedman, *The Evolution of Nuclear Strategy*, 253; Kennan, *Russia, the Atom, and the West*, 54.

[255] Donald Kagan, *On the Origins of War and the Preservation of Peace* (New York: Doubleday, 1995), 321.

[256] Robert McNamara, Secretary of Defense, "Mutual Deterrence," San Francisco, September 18, 1967, accessed January 17, 2018, http://www.atomicarchive.com/Docs/Deterrence/Deterrence.shtml.

also be credible."[257] Assured destruction evolved into MAD due to the need to build first-strike weapons to have a credible assured destruction threat. McNamara further discussed how assured destruction led to MAD: "a potential aggressor must believe that our assured-destruction capability is in fact actual, and that our will to use it in retaliation to an attack is unwavering. The conclusion, then, is clear: if the United States is to deter a nuclear attack in itself or its allies, it must possess an actual and a credible assured-destruction capability."[258] The stability of MAD-based policy was based on mutual vulnerability.[259] Missile defense systems decreased vulnerability and were a threat to MAD. Sean Kalic argues that "the whole concept of MAD rested upon the mutual vulnerability of both sides. If one side suddenly possessed the technology to render itself invulnerable to the ICBMs of the other, the whole concept of mutual assured destruction would crumble."[260] Jerome B. Wiesner and Herbert F. York, in 1964, argued that the development of ABMs could destabilize United States and Soviet tensions.[261] Wiesner and York said: "paradoxically, one of the potential destabilizing elements in the present nuclear standoff is the possibility that one of the rival powers might develop a successful

[257] McNamara, Secretary of Defense, "Mutual Deterrence."

[258] Ibid.

[259] Ibid.

[260] Sean N. Kalic, "Europe and Reagan's SDI Announcement," in *The Crisis of Détente in Europe: From Helsinki to Gorbachev*, ed. Leopoldo Nuti (New York: Routledge, 2009), 106.

[261] York and Wiesner, "National Security and the Nuclear Test Ban."

antimissile defense.[262] George F. Kennan further agreed that missile defense systems were not just destabilizing regarding nuclear relationships, but for humanity as a whole:

> The technological realities of this competition are constantly changing from month to month and from year to year. Are we to flee like haunted creatures from one defensive device to another, each more costly and humiliating than the one before, cowering underground one day, breaking up our cities the next, attempting to surrounding ourselves with elaborate shields the third, concerned only to prolong the length of our lives while sacrificing all the values for which it might be worthwhile to live at all.[263]

Kalic, Wiesner, York, and Kennan made it clear that ABM systems were a threat to MAD and could result in instability between the United States and the Soviet Union. Defenses erected in cyberspace, unlike ABM systems, would not result in the instability of international security. MAD led to the idea that SNFs were akin to bargaining chips which reduced their credibility and value as deterrents. The credible threat of force (whether first-strike or retaliatory) guided Cold War nuclear strategy. In cyberspace, the potential use of force does not warrant a MAD-based policy. Thomas Rid made the point that "if the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria."[264] Rid's contention is that the use of force in a cyberwar is "likely to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties."[265] Force in cyberspace

---

[262] York and Wiesner, "National Security and the Nuclear Test Ban."

[263] Kennan, *Russia, the Atom, and the West*, 54.

[264] Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no. 1 (2011): 10, accessed October 29, 2017, doi: 10.1080/01402390.2011.608939.

[265] Ibid., 9.

can result in "economic consequences without violent effects that then could exceed the harm of an otherwise smaller physical attack"[266] An act of cyber war can cause destructive consequences, but not to the same extent as a nuclear weapon. Emilio Iasiello argued that cyber effects have yet to reach a level of destruction commensurate with the physical use of force: "there has been no awe inspiring, game changing show of what a cyber attack can do; while incidents like STUXNET and the wiper malware that destroyed 30,000 hard drives for the Saudi oil company Saudi Aramco were significant disruptions, they were not enough to severely impact operations at either the nuclear facility or the oil company."[267] MAD, though important for understanding Cold War nuclear strategy, does not apply to cyber security strategy. The argument that missile defense systems destabilized MAD has an inherent assumption that BMDs would be effective at denying an enemy nuclear attack. Hans A. Bethe argued that, even if BMDs worked at their optimal capacity, they would still not protect a state against a nuclear attack.[268]

Bethe's argument against terminal defense systems is also an argument against strongpoint defense. Bethe thought that "terminal defense has a vulnerability all its

---

[266] Rid, "Cyber War Will Not Take Place," 9.

[267] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2013): 61, accessed October 29, 2017, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1337&context=jss.

[268] Hans A. Bethe, "Countermeasures to ABM Systems," in *ABM: An Evaluation of the Decision to Deploy an Antiballistic Missile System*, eds. Abram Chayes and Jerome B. Wiesner (New York: Harper & Row, 1969), 142.

own."[269] Bethe's point is that because a terminal defense system "defends only a small area, it can easily be bypassed."[270] Bethe gave a hypothetical example of a missile defense system that protected the largest twenty cities in the United States.[271] Then he said "it would be easy for an enemy to attack the twenty-first largest city and as many other undefended cities as he chose."[272] Bethe's point was that a strongpoint or terminal defense, because it only defends finite areas, is ineffective because all of the areas not defended are potential targets for the enemy.[273] Bethe further argues that "although the population per target would be less than if the largest cities were attacked, casualties would still be heavy. Alternatively, the offense could concentrate on just a few of the twenty largest cities and exhaust their supply of antimissile missiles, which could readily be done by the use of multiple warheads even without decoys."[274] Bethe makes an interesting point about focused defense and its vulnerabilities. Focused defense, if it is static, is also susceptible to a larger enemy concertation of forces. Bethe's argument about a focused defense being vulnerable both to overwhelming offensive firepower and susceptible to damage in undefended areas is valid for defending a city against a nuclear attack, and valid in cyberspace if one uses a strongpoint defense to secure information. Strongpoint defenses are ineffective if the enemy has a large enough attack capability.

---

[269] Bethe, "Countermeasures to ABM Systems," 142.

[270] Ibid.

[271] Ibid.

[272] Ibid.

[273] Ibid.

[274] Ibid.

The difference between digital information and a city is that digital information can be constantly sheltered, concealed, and mobile to prevent an enemy from massing his attack power. Cyber strategists must learn from Bethe's analysis that defending massive, known static location with a terminal defense system is ineffective. Whether through brute force or subversion, the enemy can still break through the defense.

Conclusion

Shelter, concealment, mobility, and dispersion, combined with ABMs, formed the basis of Cold War missile defense theory and practice. Both the United States and the Soviet Union realized they could not defend all of their SNF, so they allocated their missile defense to infrastructure they deemed critical to their national defense. In cyberspace, the United States has finite resources it must use to defend against potential malicious actors that have damaging offensive cyberweapons. With the knowledge that the United States cannot stop every cyberattack at the point of origin, it must leverage the Cold War concepts of shelter, concealment, mobility, and dispersion to defend its critical infrastructure. There is no cyberspace equivalent to an ABM which means leveraging shelter, concealment, mobility, and dispersion to defend cyber infrastructure is all the more important. When translated to cyberspace, shelter is encryption, mobility and dispersion are decentralization, and concealment remains the same. Leveraging encryption, decentralization, and concealment, cyber strategists have the foundation of a cyber deterrence strategy. Critical infrastructure in cyberspace is digital, and not physical like that of Cold War missile defense. Cyber strategists must learn from Cold War missile defense, and find the best balance to encrypt, decentralize, and conceal its digital infrastructure critical to national security. Studying Cold War theory resulted in general

principles applicable to cyber deterrence. Further exploring BMD implementation can inform cyber policymakers about specific considerations one must take when developing defensive measures in an environment dominated by the offense.

Operation Safeguard and the Strategic Defense Initiative (SDI) are two examples of missile defense systems developed by the United States during the Cold War. Operation Safeguard and SDI represent the application of shelter, concealment, mobility, and dispersion coupled with kinetic missile defense. Both Operation Safeguard and SDI show how the United States allocated its finite resources in an attempt to create a strongpoint missile defense. Operation and Safeguard and SDI had varied levels of success. The successes and failures of Operation Safeguard and SDI inform the cybersecurity strategist of general principles and pitfalls associated with a strongpoint defense against strong offensive capabilities.

CHAPTER 3

CURRENT CYBER LANDSCAPE AND THE STRATEGIC DEFENSIVE INITIATIVE

Background

> It seems highly improbable that an effective boost-phase Ballistic Missile Defense could ever be deployed. It's not that our technology, ingenuity, and creativity cannot overcome staggering obstacles. They can. It's rather that the new technology is also available to the offense for counter-measures and improved offensive weapons. These tend to be available more easily, more quickly, and much more affordable than the defenses they must overcome. What's more, in the game of countermeasures, counter-countermeasures, counter-counter-counters, etc., the tremendous destructive power of nuclear weapons gives the offense the advantage. For the offense has to overcome only a small part of the defense to succeed, while success for the defense demands near perfection.
>
> —Robert Bowman, *Star Wars: Defense or Death Star*

Unlike nuclear attacks, cyberattacks occur constantly. Joseph Nye points out that "millions of cyberattacks occur every year against all sorts of targets" and that "the Pentagon alone reports more than 10 million efforts at intrusion each day. Most are trivial, but some are costly, disruptive, and annoying to their targets."[275] The Pentagon is not the only organization targeted by cyberattacks. Strategist P.W. Singer and Allen Friedman, Director of Cybersecurity Initiatives at National Telecommunications and Information Administration in the US Department of Commerce, reported that "97 percent of Fortune 500 companies have been hacked (and 3 percent likely have been too and just don't know it), and more than one hundred governments are gearing up to fight

[275] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 47.

battles in the online domain."[276] The rate at which cyberattacks evolve means that "any great strategic advantages a nation is able to seize in a cyber arms race will be fleeting."[277] Following World War II, "the United States only had a window of four years before the Soviets were able to build their own bomb" and "that seemed incredibly quick at the time."[278] In comparison to nuclear weapons, "the proliferation of cyber weapons happens at Internet speed, so that any window that first users had with weapons like Stuxnet has already closed."[279]

The potential for a cyber-attack "on critical American infrastructure or on major financial interests that would gravely impact daily life in the US is both very real and very present."[280] Uri Tor, research fellow in the Comparative National Security Project at the Interdisciplinary Center, Herzliya, Israel, argues that "this new reality calls for a fundamental shift with respect to national security in the cyber domain, to account for the inevitability of ongoing cyber-attacks."[281] To develop an effective national security strategy in the face of persistent cyber-attacks, policymakers must understand why the offense has the advantage in cyberspace and the gap that exists between the current cyber operating environment and the most recent United States cybersecurity strategy. Because

---

[276] Friedman and Singer, *Cybersecurity and Cyberwar*, 2.

[277] Ibid., 161.

[278] Ibid.

[279] Ibid.

[280] Uri Tor, "Cumulative Deterrence as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies* 40, no. 1 (2017): 111, accessed November 25, 2017, doi:10.1080/0140202390.2015.1115975.

[281] Ibid.

cyberspace is so new, policymakers can benefit from a historical example focused defense of critical infrastructure when the offense had the advantage. The best historical example from which policymakers can learn is Ronald Reagan's decision to launch SDI in 1983.

The current environment in cyberspace regarding offensive advantage and evolving technology mirrors the challenges faced in the first years of Reagan's presidency. Reagan thought it inconceivable "that we can go on thinking down the future, not only for ourselves and our lifetime but for other generations, that the great nations of the world will sit here, like people facing themselves across a table [sic], each with a cocked gun and no one knowing whether someone must tighten their finger on the trigger."[282] Reagan's analogy of people facing each other was meant to represent state powers with nuclear weapons, but his observations stemming from the loaded-gun analogy directly correlates to the current problems in cyberspace with the proliferation of offensive cyber capability. Reagan said:

> There is one way, and that way we're pursuing, which is to see if we can get mutual agreement to reduce these weapons and, hopefully, to eliminate them, as we're trying in INF. There is another way, and that is if we could, the same scientists who gave us this kind of destructive power, if they could turn their talent to the job of, perhaps, coming up with something that would render these weapons obsolete. And I don't know how long it's going to take, but were going to start.[283]

Reagan recognized that the technology did not exist for an impenetrable nuclear defense, so the options were to have everyone with nuclear weapons agree to reduce and

---

[282] Frances Fitzgerald, *Way Out There in the Blue: Reagan, Star Wars, and the End of the Cold War* (New York: Simon and Schuster, 2000), 208.

[283] Ibid.

eventually eliminate their stockpiles, or to make a defense so strong that it would render nuclear weapons obsolete. [284] Reagan, like policymakers now, understood that it was unrealistic to expect every country with nuclear weapons to give them up voluntarily, so he pushed for the development of a strong defense to eliminate nuclear weapons.[285] In fact, Mikhail Gorbachev offered the elimination of all nuclear weapons contingent upon "banning the further development of SDI."[286] However, Reagan "saw SDI as necessary to ensure a safe transition to a non-nuclear world" and "refused to relinquish" SDI which was a major strategic gamble.[287] The United States was unwilling to lay down its nuclear weapons when given the chance. In cyberspace, it is impossible to force all potential actors to get rid of their cyber weapons, so the best option is to find a way to develop a strong defense around prioritized critical infrastructure. A defense prioritized around critical infrastructure that denies remote access to malicious actors using offensive cyber weapons greatly increases a network's security posture.[288] Understanding the situation Reagan faced and his eventual decision to begin the SDI aids in understanding the current cybersecurity issues faced by policymakers. SDI represents an attempt to develop an

---

[284] Fitzgerald, *Way Out There in the Blue: Reagan,* 208.

[285] Ibid.

[286] Gaddis*, Strategies of Containment*, 365-366.

[287] Ibid.

[288] Centre for the Protection of National Infrastructure (CPNI), "Configuring and Managing Remote Access for Industrial Control Systems," (project report, CPNI, United Kingdom, November 2010), 34-35, accessed December 30, 2017, https://scadahacker.com/library/Documents/Best_Practices/DHS%20-%20Remote%20Access%20for%20ICS.pdf.

impenetrable defense with technology that did not yet exist in an environment which favored a strong offense and actors unwilling to relinquish their weapons.[289]

Offensive Advantage in Cyberspace

The potential attacker has the advantage over the defender in cyberspace. The strength of offense in cyberspace coupled with the ubiquity of cyber-attacks creates major problems for the defender. Lawrence Freedman recognizes the prevalence of cyberattacks to include the continued back and forth between the offense and the defense: "hostile activity in the cyberdomain, represented by a continuing offensive-defensive duel, is now constant and ubiquitous. It involves activists, terrorist and criminal organizations and poses constant trouble for those trying to preserve the integrity and the effectiveness of vital networks."[290] Freedman identified the duel between offense and defense, but did not discuss the marked advantage the offense maintains in the cyber environment.[291] Joseph Nye makes it clear that "cyber defenses are notoriously porous, and the conventional wisdom holds that offense dominates defense."[292] In 2010, the Center for Strategic and Budgetary Assessments (CSBA), published a report that found "the cyber competition will be offense-dominant for the foreseeable future."[293] The CSBA further observed that

---

[289] Gaddis, *Strategies of Containment*, 365-366; Fitzgerald, *Way Out There in the Blue*, 208.

[290] Freedman, "Beyond Surprise Attack," 12.

[291] Ibid.

[292] Nye Jr., "Deterrence and Dissuasion in Cyberspace," 56.

[293] van Tol et al., *AirSea Battle: A Point-of-Departure Operational Concept*, 35.

"it will be cheaper and easier to attack information systems than it will be to detect and defend against attacks."[294] Furthermore, the Center for a New American Security (CNAS) confirmed the CSBA's research showing the offense has the advantage in cyberspace. CNAS analysis confirmed that "untraceable attackers spending hundreds, thousands, or millions of dollars possess a clear advantage over defenders spending billions of dollars on cyber defenses that do not offer reliable protection."[295] CNAS "calculated that a high-end 'cyber army' capable of overcoming U.S. government defenses could be developed in two years for 100 million dollars, a fraction of the amount that the United States spends on cybersecurity each year.[296] In a report prepared for the United States Department of Energy, The Pacific Northwest National Laboratory (PNNL) reinforced the strength of the offense in cyberspace:

> The advantage in the cyber domain, as in the nuclear domain, favors the offense. A defender must block all attacks, while the attacker only needs to be successful once. At the same time, unlike in the nuclear domain where the arsenal is finite and costly and each weapon can be used only once, there is little to deter an attacker from mounting a continual barrage of cyber-attacks given the low cost of doing so.[297]

---

[294] van Tol et al., *AirSea Battle: A Point-of-Departure Operational Concept*, 35.

[295] Kristin M. Lord and Travis Sharp, ed., "America's Cyber Future: Security and Prosperity in the Information Age: Volume 1," (project report, Center for a New American Security, Washington, DC, June 2011), 28, accessed November 25, 2017, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238.

[296] Ibid.

[297] Pacific Northwest National Laboratory, "Cyber Deterrence and Stability: Assessing Cyber Weapons Analogous through Existing WMD Deterrence and Arms Control Regimes," (project report, Pacific Northwest National Laboratory, Alexandria, VA, September 2017), 1.21, accessed November 26, 2017, http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26932.pdf.

PNNL's report, authored by nonproliferation and policy analyst Rustam Goychayev, cybersecurity researcher Sam Clements, and eight other cyber and non-proliferation researchers highlighted the limited ability of a defender to deter an attacker from launching continual cyber-attacks because cyber-weapons are not one-use weapons, like a nuclear warhead.[298] Kristin Lord, Vice President and Director of Studies at CNAS, and Travis Sharp, non-resident fellow at the Modern War Institute, argued that the reason that the offensive has the advantage is not just because of the "favorable cost ratio" compared to the defender, but also because "attackers also possess advantages in the required levels of effort and complexity."[299] Lord and Sharp accurately identify that an attacker can conduct a cyberattack with less money, complexity, and effort than the defender trying to protect the network.[300]

In 2011, Regina E. Dugan, the Defense Advanced Research Projects Agency (DARPA) director, submitted testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities in which she highlighted the advantage of the offense in cyberspace. Dugan posited that the number of lines of code included in security software increased from several thousand twenty years ago to nearly 10 million today. Over the same period, the number of lines of code included in malware

[298] There are cyber weapons, specifically zero-day exploits, that are one-shot weapons because once they are employed the defender can patch his systems and thus be invulnerable to that specific exploit. But, zero-day exploits are cheap and easily attainable so the cost of deploying one is negligible and new zero-day exploits are discovered daily.

[299] Ibid., 28.

[300] Ibid.

remained constant at approximately 125.[301] Lord and Sharp summed up Dugan's testimony and said: "cyber defenses have grown exponentially in effort and complexity, but they continue to be defeated by offenses that require far less investment by the attacker."[302] The 2017 report prepared by the Defense Science Board (DSB) Task Force on Cyber Deterrence reinforced Dugan's 2011 testimony. The DSB Task Force concluded in their opening memorandum to their report that "the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries."[303] Game-theory based analysis of cybersecurity recognizes that "attackers are constantly escalating their attack power and sophistication," while defenders are not increasing their defense power and sophistication at the same rate.[304] Cyber scholars Lu Wenlian, Shouhaui Xu, and Xinlei

[301] U.S. Congress, House, Defense Advanced Research Projects Agency Director Regina E. Dugan, *Testimony before the House Armed Services Committee*, Subcommittee on Emerging Threats and Capabilities, Washington, DC, 1 March 2011, 16-17, accessed January 17, 2018, https://www.darpa.mil/attachments/TestimonyArchived%20(March%201%202011).pdf.

[302] Lord and Sharp, "America's Cyber Future: Security and Prosperity in the Information Age: Volume 1," 28.

[303] DoD Defense Science Board, *Task Force on Cyber Deterrence*.

[304] Ren Zheng, Wenlian Lu, and Shouhuai Xu, "Optimizing Active Cyber Defense" (paper presented at Proceedings of the 4th Conference on Decision and Game Theory for Security, 2016), 206, accessed November 25, 2017, arXiv:1603.08312 [cs.CR].

Yi[305] argued "the effect of malware-like attacks is automatically amplified by the network connectivity, while the defense effect is not."[306] Consulting and research development organizations Smart Information Flow Technologies (SIFT), Dynamic Object Language Labs (DOLL), and Bobrow Computational Intelligence co-wrote a paper in which they argue that "present day cyber defense systems rely on fixed sets of sensors" that "have a limited set of types" and are "unable to incorporate information about the network in which they are installed."[307]

Cyber defenders not only have to spend more time and resources than the attacker, they also have to compete against the attacker's superior ability to leverage the strength of connected networks. Often defenders in cyberspace implement static security measures, which means an attacker only requires one evolution of their cyberattack to make an existing cyber defense obsolete.[308] Where an attacker can constantly probe a system and conduct iterative attacks until a cyber payload penetrates the defense, most current cyber defenses only screen against known vulnerabilities and malware which

[305] Lu Wenlian is a professor at Fudan University in China and a Marie Curie Research Fellow at the University of Warwick in the United Kingdom. Shouhaui Xu is a Professor in the Department of Computer Science, University of Texas San Antonio, and the Director of the Laboratory for Cybersecurity Dynamics. Xinlei Yi is a doctoral student in the Fudan University School of Mathematical Sciences.

[306] Ibid., 206.

[307] J. Benton, Robert P. Goldman, Mark Burstein, Joseph Mueller, Paul Robertson, Dan Cerys, Andreas Hoffman, and Rusty Bobrow, "Active Perception for Cyber Intrusion Detection and Defense" (paper presented at The Workshops of the Thirtieth AAAI Conference on Artificial Intelligence Artificial Intelligence for Cyber Security: Technical Report WS-16-03, Cambridge, MA, September 21-25, 2013), 157, accessed November 26, 2017, doi: 10.1109/SASOW.2015.20.

[308] Zheng, Lu, and Xu, "Optimizing Active Cyber Defense," 206.

does not account for undiscovered vulnerabilities or a new iteration of malware.[309] With the knowledge that cyberspace currently favors the offense, comparing the United States' cybersecurity strategy to the known defensive capability gaps (cost, complexity, and leveraging a connected system) will reveal opportunities that the United States can use to strengthen its cybersecurity strategy.

United States Cybersecurity Strategy

The DoD "defend [s] DoD networks, systems, and information; defend[s] the nation against cyberattacks of significant consequence; and support[s] operational and contingency plans."[310] DoD's current cyber strategy states: "the United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential future attack if it penetrates the United States' defenses."[311] DoD emphasizes United States response capabilities to a cyberattack as a deterrent to potential attackers.[312] The Department of Defense's cyber strategy also emphasizes defense by denial and says "[the] DoD must increase its defensive capabilities to defend DoD networks and defend

[309] Benton et al., "Active Perception for Cyber Intrusion Detection and Defense," 157.

[310] DoD, *The Department of Defense Cyber Strategy*, 3.

[311] Ibid., 11.

[312] DoD, *The Department of Defense Cyber Strategy*, 3.

the nation from sophisticated cyber-attacks."[313] Furthermore, the Department of Defense argues that deterrence by denial is strengthened with cooperation between "other departments, agencies, international allies and partners, and the private sector."[314] The existing Department of Defense strategy for cybersecurity does not prioritize the critical infrastructure that must be protected by cyber denial, but it does recognize that cyber denial does not apply to all of cyberspace. Current Department of Defense cybersecurity strategy identifies that the United States should prioritize and defends its most important networks: "while DoD cannot defend every network and system against every kind of intrusion – DoD's total network attack surface is too large to defend against all threats and too vast to close all vulnerabilities – DoD must take steps to identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively."[315] In their cybersecurity strategy, DoD identifies that a perimeter cyber defense is not possible because of existing vulnerabilities, but that it must conduct strongpoint defense by defending its most critical cyber infrastructure so that it can effectively continue operations.[316] The United States is under no illusion that deterrence by denial is always effective and recognizes that strategies must be in place when deterrence by denial fails.[317]

---

[313] Ibid.

[314] Ibid.

[315] Ibid., 13.

[316] DoD, *The Department of Defense Cyber Strategy*, 13.

[317] Trump, *National Security Strategy of the United States*, 13.

The Department of Defense says its existing "capabilities cannot necessarily guarantee that every cyberattack will be denied successfully," which means the Department of Defense "must invest in resilient and redundant systems so that it may continue its operations in the face of disruptive or destructive cyberattacks on DoD networks."[318] DoD's cyber strategy also claims that "effective resilience measures can help convince potential adversaries of the futility of commencing cyberattacks on U.S. networks and systems."[319] Current Department of Defense cyber strategy briefly describes how "a potential adversary need not spend billions of dollars to develop an offensive capability," but does not address how a defense-focused cyber strategy could overcome issues of cost, complexity, and an inability to leverage the strength of a connected system.[320] Currently, DoD's strategy is incomplete because it does not address the most challenging issues (cost, complexity, and leveraging the network to adapt) of implementing cyber deterrence and conducting deterrence by denial. Cyberspace is a new domain, and thus there is no precedent from which policymakers can turn for advice on strategy development. Identifying and analyzing SDI provides a foundation from which cyber policymakers can build an effective cyber defense strategy.

Reagan's decision to implement SDI is the most analogous case study from which cyber policymakers can learn about the development of a defense-first strategy aimed at making the continued evolution of weapons obsolete. Reagan was faced with an

[318] Ibid., 11.

[319] Ibid.

[320] Ibid., 9-10.

environment in which "the idea of building strategic defenses had virtually no constituency in the Pentagon."[321] Safeguard, the most recent failed ABM system, cost six billion dollars and was only operational between April, 1975 and September, 1975.[322] Safeguard "was technologically obsolete almost as soon as it began operations."[323] Advocates of Safeguard "argued that a defensive system would render nuclear missiles obsolete, thus ending the arms race."[324] Because Safeguard focused on a static (and not evolving) defense against nuclear weapons, it did not increase United States nuclear deterrence, and did not make nuclear weapons obsolete.[325] The failure of Safeguard was still fresh in the minds of those in the Pentagon when Reagan began thinking about SDI.

Reagan recognized that no defense "could ever be expected to be one hundred percent effective," but he also thought that if a nuclear defense system worked "and we entered into an era when the nations of the world agreed to eliminate nuclear weapons, it could serve as a safety valve against cheating – or attacks by lunatics who managed to get their hands on a nuclear missile."[326] Reagan further wrote that "if we couldn't reach an agreement eliminating nuclear weapons, the system would be able to knock down enough of an enemy's missiles so that if he ever pushed the button to attack, he would be doing

---

[321] Fitzgerald, *Way Out There in the* Blue, 116.

[322] David W. Mills, *Cold War in a Cold Land: Fighting Communism on the Northern Planes* (Norman: University of Oklahoma Press, 2015), 270.

[323] Ibid.

[324] Ibid., 259.

[325] Ibid., 270-271.

[326] Fitzgerald, *Way Out There in the Blue*, 263.

so in the knowledge that his attack was unable to prevent a devastating retaliatory strike."[327] Reagan wanted to develop a nuclear defense that would compel nations to surrender their nuclear weapons, counter the ICBM threat from the Soviet Union, protect the United States from "lunatics" with nuclear weapons, and to act as a deterrent if no agreement on nuclear disarmament could be reached.[328] Reagan was also aware that the technology required to implement a legitimate defense against nuclear weapons did not yet exist.[329] The offense-dominated environment surrounding nuclear weapons before Reagan's decision to launch SDI parallels current challenges in cyberspace. The current challenge the United States faces in cyberspace is how to develop a cyber defense to deny state and nonstate actors from attacking critical infrastructure in an environment advantageous to the attacker with technology that does not yet exist.

President Reagan and the Strategic Defense Initiative

On March 23, 1983 President Reagan gave a speech that introduced SDI. Reagan made it clear that "defense policy of the United States is based on a simple premise: The United States does not start fights."[330] Reagan further said that because the United States is not an aggressor, "we maintain our strength in order to deter and defend against

---

[327] Ronald Reagan, *An American Life* (New York: Simon and Schuster, 1990), 608

[328] Ibid.

[329] Ibid.

[330] Ronald Reagan, Speech on 'Defense Spending and Defense Technology,' March 23, 1983, in *Office of Technology Assessment (OTA), Strategic Defenses Ballistic Missile Defense Technologies: Anti-Satellite Weapons, Countermeasures, and Arms Control*, 297-298 (Princeton, NJ: Princeton University Press, 1986).

aggression -- to preserve freedom and peace."[331]In his speech, Reagan claimed deterrence means "making sure any adversary who thinks about attacking the United States, or our allies, or our vital interest, concludes that the risks to him outweigh any potential gains" and concluded that "weakness only invites aggression."[332] Reagan then asked a rhetorical question leading up to the announcement of SDI: "What if free people could live secure in the knowledge that their security did not rest upon the threat of instant U.S. retaliation to deter a Soviet attack, that we could intercept and destroy strategic ballistic missiles before they reached our own soil or that of our allies?"[333] Reagan's rhetorical question hinted at a proactive defensive approach to nuclear missile defense that went against mutually assured destruction and instead created deterrence by a strong defense.[334] Reagan then discussed the technological difficulty of meeting his vision of a proactive nuclear defense. He stated:

> I know this is a formidable, technical task, one that may not be accomplished before the end of the century. Yet, current technology has attained a level of sophistication where it's reasonable for us to begin this effort. It will take years, probably decades of efforts on many fronts. There will be failures and setbacks, just as there will be successes and breakthroughs. And as we proceed, we must remain constant in preserving the nuclear deterrent and maintaining a solid capability for flexible response. But isn't it worth every investment necessary to free the world from the threat of nuclear war? We know it is.[335]

---

[331] Ibid.

[332] Ibid.

[333] Ibid.

[334] Ibid.

[335] Reagan, Speech on 'Defense Spending and Defense Technology.'

In a nuclear environment where the offense was superior to the defense, Reagan recognized that developing the technology to meet his vision of a proactive nuclear defense took time. Reagan called "upon the scientific community" in order "to turn their great talents now to the cause of mankind world peace" and to give the United States "the means of rendering these nuclear weapons impotent and obsolete."[336] The strength of the SDI was that it called for research and development of the required technology, not a concrete solution. Another attempt at an ABM solution would likely have failed just like Safeguard because the offensive capability of the Soviet Union would overwhelm any new static ABM system. However, by recognizing that a proper nuclear defense could take decades, Reagan created a project that involved "intensive research and development into a multi-tiered missile defense system."[337] In an offensive-dominated environment, research and development into a multi-tiered defensive solution created the potential for long term innovation and avoids the problem of allocating funds and resources to produce an iterative defense that is static and obsolete upon inception.

Nikolai V. Mikhailov, Russian Deputy Minister of Defense from 1997-2001, said one of the reasons the Soviet Union collapsed was "the [U.S.] Strategic Defense Initiative and the aspiration of the Soviet political leadership to counteract it" with an asymmetric response.[338] John Lewis Gaddis also praised SDI:

> SDI was a striking demonstration of killing multiple birds with a single stone: in one speech Reagan managed simultaneously to pre-empt the nuclear freeze movement, to raise the prospect of not just reducing but eliminating the need for

[336] Ibid.

[337] Kalic, "Europe and Reagan's SDI Announcement," 101.

[338] Gruntman, *Intercept 1961: The Birth of Soviet Missile Defense*, 91, 251.

> nuclear weapons, to reassert American technological prominence, and, by challenging the Soviet Union in an arena in which it had no hope of being able to compete, to create the strongest possible incentive for Soviet leaders to reconsider the reasons for competition in the first place.[339]

Because a research program focused on technologically advanced proactive defense played a factor in challenging the power and capability of a state actor with a strong offensive capability, it should be analyzed for applicability to cyberspace. An understanding of the framework, weaknesses, and outcomes of SDI results in lessons identified that will inform cyber policy-makers how the United States should approach a long-term approach to strategic cyber deterrence.

SDI Guidance

Historian John Prados said "the concept behind SDI – and the reason much of the public came to call it 'Star Wars' – was to craft a defense against ballistic missiles utilizing exotic technologies, lasers, or particle-beam projectors."[340] Because SDI was a research project, and the technology to implement SDI did not yet exist, Reagan needed to issue clear guidance to achieve his desired vision of a space-based proactive nuclear defense. Following his speech, Reagan "moved rapidly to concretize the Star Wars program."[341] On March 25, 1983, Reagan "signed the National Security Decision Directive (NSDD), 85 in which he authorized his national security bureaucracy to

---

[339] Gaddis, *Strategies of Containment*, 358-359

[340] John Prados, "The Strategic Defense Initiative: Between Strategy, Diplomacy and US Intelligence Estimates," in *The Crisis of Détente in Europe: From Helsinki to Gorbachev*, ed. Leopoldo Nuti (New York: Routledge, 2009), 86.

[341] Ibid., 87.

conduct research on SDI."[342] In NSDD 85, Reagan "direct[ed] the development of an intensive effort to define a long-term research and development program aimed at an ultimate goal of eliminating the threat posed by nuclear ballistic missiles."[343] Following NSDD 85, Reagan signed NSDD 6-83 which directed a study to "define a research and development program aimed at the ultimate goal of eliminating the threat posed by nuclear defensive missiles" through both a "future security strategy and a defense technology plan."[344] After he signed NSDD-83: "Reagan established the Defense Technology Oversight committee to ramp-up the research on SDI, guide the actions of the Defense Technology Study Group (later known as the Fletcher Panel) and direct the Future Security Strategy Study (or the Hoffman Panel) to begin researching SDI feasibility and technology."[345] The Hoffman Panel concluded that "US national security required the development of technical opportunities for an advanced ballistic missile defense system."[346] Sean Kalic further discussed the methodology behind the conclusions of the Hoffman Panel:

---

[342] Kalic, "Europe and Reagan's SDI Announcement," 101.

[343] Ronald Reagan, National Security Decision Directive 85, *Eliminating the Threat from Ballistic Missiles* (Washington, DC: The White House), accessed September 17, 2017, https://reaganlibrary.archives.gov/archives/reference/Scanned%20NSDDS/NSDD85.pdf.

[344] Ronald Reagan, National Security Decision Directive 6-83, *Study on Eliminating the Threat Posed by Ballistic Missiles* (Washington, DC: The White House), accessed September 17, 2017, https://catalog.archives.gov/id/6858544.

[345] Kalic, "Europe and Reagan's SDI Announcement," 101.

[346] 'Ballistic Missile Defenses and US National Security' (Hoffman Report), October 1983, reproduced in S. E. Miller and S. Van Evera eds., *The Star Wars Controversy* (Princeton, NJ: Princeton University Press, 1986), 219.

> The Hoffman panel based its conclusions on the Soviet Union's continued construction and deployment of 'nuclear offensive forces.' The panel's members believed that if the Soviet Union continued on their course of modernization, the credibility of America's nuclear deterrent would be significantly eroded. The Hoffman Panel asserted that the deployment of a strategic defense, combined with nuclear force modernization programs, would enhance the withering nuclear deterrent of the United States.[347]

The Hoffman Panel's conclusion completed the "Future Security Strategy Study" outlined in NSDD 6-83. The Fletcher panel completed the "Defense Technology Study Group" portion of NSDD 6-83 6 months after the Hoffman Panel.

The Fletcher Panel concluded that "advanced technologies in surveillance, acquisition, tracking, and direct energy weapons, conventional weapons, battle management, and data processing enabled the United States to begin intensive research and development into a multi-tiered missile defense system."[348] NSDD 85, NSDD 6-83, the Hoffman Panel, and the Fletcher Panel were the foundation of SDI. Reagan used NSDD 85 and 6-83 to direct his intent, and the Hoffman and Fletcher Panels conducted the research to determine the viability of Reagan's vision. Reagan did not assume SDI was possible, but instead directed scientists and policymakers to determine the viability of SDI as a defense strategy, and to determine if existing technology was advanced enough to begin research. The Hoffman Panel concluded that SDI was viable as a defense strategy and the Fletcher Panel concluded that existing technology was advanced enough to begin research and development for SDI.[349] A future defense solution in cyberspace requires the same type of scientific inquiry Reagan directed in NSDD 85 and NSDD 6-

---

[347] Kalic, "Europe and Reagan's SDI Announcement," 101.

[348] Ibid.

[349] Kalic, "Europe and Reagan's SDI Announcement," 101.

83. Cyber policymakers must ask the same questions as Reagan. First, is cyber deterrence a feasible and viable national defense strategy in a future dominated by cyber offense. Second, does the technology currently exist to begin research and development of a proactive cyber defense solution. Though SDI was a promising research project, it still had many critics that were quick to point out its shortcomings and long-term viability.

Weaknesses of SDI

Dr. Bowman, former President of the Institute for Space and Security Studies, wrote an entire book dedicated to critiquing the vision of SDI. Bowman's *Defense or Death Star* contains criticism from which cyber policymakers can learn when developing a long-term solution for strategic cyber deterrence. Bowman has many criticisms of SDI, but the criticism most applicable to strategic cyber defense centers on the location of the defender during boost-phase intercept, the offense still having the advantage in cost and complexity, and attacks that evade a proactive defense system.

One of the capabilities envisioned by researchers working on SDI was the ability to intercept an ICBM at the boost-phase from space because "boosters under power have flaming exhaust tails which are easy to detect and track with heat-seeking IR sensors, even from satellites 20,000 miles or so away."[350] Bowman identified that "the boost phase lasts only a short time (40 to 300 seconds), and it occurs very near the launch point. Therefore, an intercept must occur over enemy territory (or, for SLBMs, over the ocean). This requirement very much complicates the basing of a defensive system."[351] A

[350] Bowman, *Star Wars: Defense or Death Star?,* 15.

[351] Ibid., 16.

proactive defense that must reside over enemy territory directly correlates to Defensive Cyber Operations – Response Actions (DCO-RA). In the United States Army War College's 2016 Strategic Operations Cyber Guide, there is a definition of DCO-RA that involves defense measures external to the Department of Defense Information Networks (DODIN):

> DCO-RA are those deliberate, authorized defensive actions which are taken external to the DODIN to defeat ongoing or imminent threats to defend DOD cyberspace capabilities or other designated systems. DCO-RA must be authorized in accordance with (IAW) the standing rules of engagement and any applicable supplemental rules of engagement and may rise to the level of use of force. In some cases, countermeasures are all that is required, but as in the physical domains, the effects of countermeasures are limited and will typically only degrade, not defeat, an adversary's activities.[352]

DoD's cyber strategy using DCO-RA has a similar problem to SDI; intercept of an enemy cyberattack must occur in enemy cyber territory. Just like a nuclear weapon, a cyberattack is much more difficult to stop once it leaves its point of origin and enters cyberspace. Bowman cautioned that SDI was in fact an offensive system masquerading as a defensive system.[353] Cyber policy-makers that want to implement pro-active cyber defense in enemy cyber territory must balance a fine line between what constitutes active defense of critical infrastructure and a pre-emptive first strike. Bowman further argued that placing a defense system in space, with a constant orbit, would drive up the costs and complexity of the defender compared to the attacker.[354]

---

[352] United States Army War College, *Strategic Cyberspace Operations Guide* (Carlisle, PA: U.S. Army War College, 2016), 17, accessed December 7, 2017, https://www.csl.army.mil/usacsl/Publications/Strategic_Cyberspace_Operations_Guide_1_June_2016.pdf.

[353] Bowman, *Star Wars: Defense or Death Star?,* 78-79.

[354] Ibid., 18, 28.

Bowman's analysis of the SDI concept showed that, even with the most current technology, the attacker still had the advantage. Bowman, discussing space-based missile defense platforms, explained:

> They can't just stand there, but must orbit the earth at a velocity dependent on the altitude. Any given component (laser battle station, machine gun, or whatever) spends only a fraction of the time within range of the missile fields where boost phase will occur. This means that, depending on the lethal range of the particular weapons being used, there must be ten to thirty components in orbit for every one actually on station. The fact does not disprove the technical feasibility of such defenses, but certainly influences the economic tradeoffs between the offense and defense. The offense can drive up the number of 'Star Wars' battle stations required, and therefore the cost of the defenses, by increasing the number of offensive boosters to be intercepted, by hardening the boosters to decrease the lethal range of each defensive weapon, by modifying the boosters to shorten the vulnerable boost time, or by some combination of these.[355]

Bowman reinforced his argument about the disadvantage of the defender under SDI and claimed new technology is available "for the offense for counter-measures and improved offensive weapons" which "tend to be available more easily, more quickly, and more affordably than the defenses must overcome."[356] Bowman's argument for the offense's advantage, even with the vision for SDI fully realized, must influence cyber policymakers. The strongest defense is vulnerable to a persistent attacker which means cyber policymakers must identify vulnerabilities, decide where to assume risk, and develop response measures to effectively defend critical infrastructure. If cyber policy attempts to use static measures to police and defend the entirety of cyberspace, the

[355] Ibid., 18.

[356] Bowman, *Star Wars: Defense or Death Star?,* 28.

attacker will always have the advantage.[357] A strategic cyber defense is not constrained as much as the vision of SDI which involved a physical defense located in a predictable orbit. Bowman's critique of a static system requiring continued upgrading does not apply to cyberspace if the attacker does not know where the defender is located. Static cyber defense aimed at defeating proactively an enemy attack at its point of origin will fail because the attacker will adapt to the defender and overcome the defense.[358] Cyber policymakers must learn from the weaknesses of SDI and ensure any proactive defense is encrypted, decentralized, and concealed (similar principles as the location of SNF: sheltered, mobile, and concealed). Bowman also brought up the possibility of attacks that evade proactive defense measures similar to spoofing or insider attacks in cyberspace.

Bowman did not think an impenetrable SDI was possible but made the argument that even if SDI worked perfectly, it still could not stop a nuclear attack. Bowman argued:

> even if a totally impregnable, invulnerable 'Star Wars' system could be deployed – one capable of destroying all ICBMs in flight – it would be of little or no strategic value, because it could not prevent nuclear weapons from being delivered by other means. Ballistic missiles can be launched by submarines from fairly short range. These missiles can use low-angle trajectories such that their entire flight – not just the boost phase – lies within the protective blanket of the atmosphere.[359]

---

[357] Sridhar Venkatesan, Massimiliano Albanese, George Cybenko, Sushil Jajodia, "A Moving Target Defense Approach to Disrupting Stealth Botnets" (paper presented at Proceedings of the 2016 ACM Workshop on Moving Target Defense), 40-45, accessed December 30, 2017, https://www.researchgate.net/profile/Massimiliano_Albanese/publication/310821206_A_Moving_Target_Defense_Approach_to_Disrupting_Stealthy_Botnets/links/592b3fe9a6fdcc44435b11e6/A-Moving-Target-Defense-Approach-to-Disrupting-Stealthy-Botnets.pdf.

[358] Zheng, Lu, and Xu, "Optimizing Active Cyber Defense," 206.

[359] Bowman, *Star Wars: Defense or Death Star?,* 29.

Bowman's argument that even a perfect space-based nuclear defense could not prevent nuclear weapons because of obfuscated launch angles and trajectories mirrors the problem of cyber defenses where an attacker can obfuscate a cyberattack to bypass the defense. Obfuscation can occur in any code. A 2013 paper presented by professors Xun Lu, Jianwei Zhuge, Rouyu Wan, Yinzhi Cao, and Yan Chen from the Institute of Network Science and Cyberspace, Tsinghua University (Beijing, China) at the 46th International Conference on System Sciences discussed how hackers had the ability to obfuscate malicious code in Adobe Files.[360] Adobe Reader is valuable as an example because it is the primary format used in the DoD for personnel files. PDFs are a popular format and have a "complexity of rich features allowed by Adobe Reader (the most widely used PDF viewer)."[361] In 2013, Adobe Reader had software that "boost[ed] the functionality of PDF document[s]" and allowed "PDF[s] to perform tasks such as validation and calculation."[362] The problem with the software Adobe used, was that it also "bestow[ed] upon attackers the power to run arbitrary code by exploiting vulnerabilities" in Adobe's software.[363] Adobe's 2013 vulnerability highlights the "simplicity of malicious code development and the effectiveness of obfuscation

[360] Xun Lu, Jianwei Zhuge, Ruoyu Wan., Yinzhi Cao, and Yan Chen, "De-Obfuscation and Detection of Malicious PDF Files with High Accuracy" (paper presented at the 46th Hawaii International Conference on System Sciences, 7-10 January 2013), 2, accessed February 13, 2018 https://doi.org/10.1109/HICSS.2013.166.

[361] Lu et al., "De-Obfuscation and Detection of Malicious PDF Files with High Accuracy," 7-10.

[362] Ibid.

[363] Ibid.

mechanisms" whose aim is to generate, "from already existing code, a new application that cannot be assed yet as being risky by security controls."[364] Because most of the "codes embedded in malicious PDFs [were] extensively obfuscated," cyber defenses had trouble analyzing a PDF's code for discrepancies and "anti-virus applications [were] not able to cope with even the most well-known PDF vulnerability."[365]

The example with Adobe PDFs in 2013 shows how attackers using cyber weapons can circumvent seemingly perfect cyber defenses by obfuscating their attacks. Bowman warned that an attacker could disguise nuclear attacks through varying launch angles and trajectories which directly applies to cyber defense where an attacker can disguise or mask his cyber weapon to thwart a seemingly perfect defense. The lesson for cyber planners is that any defense has vulnerabilities, the important part of a cyber defense strategy is to shape the cyber operating environment so that a defender's vulnerabilities require time and resources to exploit thus increasing the chance of attribution of the attacker. Even the best cyber defense will have a vulnerability, but a defender can still be effective if he funnels potential attackers to vulnerabilities that do not impact infrastructure critical to his national security. Bowman further highlights the difficulties in preventing insider attacks which is also a major challenge in cyberspace.

---

[364] Jasiul Bartosz, Marcin Szpyrka, and Joanna Sliwa, "Detection and Modeling of Cyber Attacks with Petri Nets," *Entropy* 16 (2014): 6603-6604, accessed January 6, 2018, doi:10.3390/e16126602.

[365] Lu et al., "De-Obfuscation and Detection of Malicious PDF Files with High Accuracy," 2.

Bowman points out that nuclear missiles do not have to be launched to be detonated.[366] Bowman says:

> Nuclear weapons can also be delivered by light aircraft, barge, sailboat, diplomatic pouch, indeed by any of the many ways people smuggle cocaine and marijuana into the country. If one is concerned with nuclear blackmail, then one must consider the threat of pre-emplaced nuclear weapons which could be detonated on command. No 'Star Wars' system can eliminate that threat. It cannot disarm potential nuclear terrorists.[367]

Bowman's discussion of pre-emplaced nuclear weapons directly correlates to the threat of pre-emplaced cyber weapons from an insider threat.[368] The United States Secret Service and Carnegie Mellon University produced a six-year joint study on insider cyber threat in which they identified that "insiders have the potential to pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases."[369] The insider threat study identified that "fifty-five percent of the organizations that were victims of electronic crime reported one or more insider incidents or intrusions, with 58% of the incidents known or suspected to have come from outsiders, 27% from insiders, and 15% from an unknown origin."[370] Unlike a pre-emplaced nuclear weapon, a pre-

---

[366] Bowman, *Star Wars: Defense or Death Star?*, 29.

[367] Ibid.

[368] Ibid.

[369] Eileen Kowalski and Dawn Cappelli, "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector," (project report, National Threat Assessment Center, Washington, DC, January 2008), 4, accessed December 7, 2017, https://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52266.pdf, 4.

[370] Ibid., 6.

emplaced cyber weapon will not cause immediate mass physical destruction.[371] Insider attacks will happen, and they will happen against infrastructure critical to the national security of the United States.

Cyber policymakers must make every effort to limit the amount of damage one can cause from an insider attack by shaping the scope of privileges afforded to those with access to critical infrastructure. Even with a perfect exterior cyber defense, an insider attack is still possible because of access and privileges given to those associated with securing critical infrastructure. Because insider attacks and pre-emplaced cyber weapons are not preventable, leadership involved with infrastructure critical to United States national security has an obligation to create a system that limits privileges so that an insider attack will cause the minimal amount of damage possible and results in immediate attribution of the perpetrator. Bowman's analysis of pre-emplaced nuclear weapons reinforces the need for cyber policymakers to account for insider risk as a major threat to critical cyber infrastructure.[372]

Bowman's analysis of SDI directly applies to cyberspace because he identifies multiple scenarios in which the defender is still at a disadvantage even with advanced technology.[373] Bowman's analysis did not discuss any potential positive outcomes of the SDI program.[374] Though Bowman focused on many negative aspects of the proposed

---

[371] Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," 61.

[372] Bowman, *Star Wars: Defense or Death Star?*, 29.

[373] Ibid.

[374] Ibid.

vision for SDI, there were many dividends of SDI that positively affected missile defense and technology development for decades.

Dividends of SDI

The priority of SDI research was on ballistic missile defense and various subcomponents, but the outcomes of SDI research extended far beyond defending the United States from nuclear weapons or even military application. Former SDI directors Henry F. Cooper and retired Air Force Lieutenant General James A. Abrahamson made it clear that SDI's "innovation translated into substantial savings" for the government as well as "remarkable hardware advances – and in electronics, sensors and detectors, computers, propulsion, communications, and power" for military and civilian organizations.[375] There are multiple positive dividends of SDI research, but two examples show how research intended for military application created unexpected positive outcomes: research into particle accelerators and research into space exploration.

SDI researchers "focused much attention on developing low-cost, reliable particle accelerators as part of a system to provide protection against ballistic missile attacks."[376]

---

[375] Henry F. Cooper and James A. Abrahamson, "The Dividends of SDI," *The Journal of International Security Affairs Symposium: Modern Missile Defense at 30* (2013): 7, accessed December 30, 2017, http://highfrontier.org/wp-content/uploads/2013/06/The-Dividends-of-SDI.pdf.

[376] Nick Montanarelli and Ted Lynch, "Applications of the Strategic Defense Initiative's Compact Accelerators" (paper presented at NASA, Washington, Technology 2001: The Second National Technology Transfer Conference and Exposition, vol. 2, 2001), 503, accessed December 30, 2017, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19920013489.pdf.

Particle accelerator research was part of SDI's "directed energy weapons program."[377] SDI researchers looked into "ways to reduce the size, weight, and cost and increase the reliability of particle accelerators that drive free electron lasers, neutral particle beams, and other directed energy weapons."[378] Researchers knew that "accelerator technology could be used for a number of medical and industrial applications" but not until the "improvements in size, weight, and cost sought by SDI" would accelerator technology benefit commercial applications.[379]

SDI particle accelerator research resulted in an improved Radio-Frequency Quadrupole linear accelerator (RFQ linac). RFQ linac technology was then used in California's Loma Linda University Medical Center in the form of proton cancer therapy.[380] AccSys Technology, Inc. "provided the RFQ linac injector" to Loma Linda University Medical Center, and "Science Applications International Corporation (SAIC) installed the entire synchrotron system."[381] Both AccSys Technology and SAIC did "extensive work on accelerators for SDI which contributed" to the commercialization of proton cancer therapy.[382] Loma Linda University still uses proton therapy to treat cancer and claims it is "the most precise and advanced form of radiation beam therapy available

---

[377] Ibid.

[378] Ibid.

[379] Ibid.

[380] Montanarelli and Lynch, "Applications of the Strategic Defense Initiative's Compact Accelerators," 504.

[381] Ibid.

[382] Ibid.

today."[383] Research intended to defeat Soviet nuclear missiles accelerated the availability of a cancer treatment method used to this day. SDI research not only led to breakthroughs in cancer treatment, but also to space exploration.

In 1991, Miles Palmer, former member of the DoD SDI rocket propulsion advisory panel, and Roger Lenard, former member of the SDI organization in charge of lightweight interceptors, correctly predicted that SDI directly applied to the future of space travel.[384] Palmer and Lenard identified that the "low-cost launch of fuel, water, and other expendables to a space station, the Moon, and Mars is shown to apply to a vigorous expansion of interplanetary missions within constrained budgets."[385] Palmer and Lenard then showed how SDI lowered the cost of space travel through research geared towards missile defense.[386] In an article for *wired.com*, United States Geological Survey Astrogeology Science Center contributor and former contract NASA historian, David S. F. Portree reinforced Palmer and Lenard's assertion and said: "neither the on-going Discovery Program of cheap, relatively frequent automated lunar and planetary missions nor the low-cost automated Mars missions of the 1996-2008 period would have been

---

[383] Loma Linda University Proton Treatment & Research Center, "What is Proton Therapy?", accessed December 30, 2017, https://protons.com/.

[384] Miles Palmer and Roger Lenard, "A Revolution in Access to Space Through Spinoffs of SDI Technology," *IEEE Transactions on Magnetics,* 27, no. 1 (1991): 11, accessed December 30, 2017, http://ieeexplore.ieee.org/document/100986/.

[385] Palmer and Lenard, "A Revolution in Access to Space Through Spinoffs of SDI Technology," 11.

[386] Ibid.

possible without the technology infusion from SDI."[387] Though focused on space operations related to replenishing a missile defense system, SDI research accelerated United States Space exploration and associated scientific research. SDI research created "technical innovations" that "would never have happened in a program with a 'business as usual' approach."[388] Cyber policymakers should follow the example set by SDI and develop a research program geared towards long-term cyber defense. Long term investment in cyber defense research creates the opportunity for the United States to effectively defend critical infrastructure for the foreseeable future and to lower the cost of emerging technology resulting in increased innovation in the commercial sector.

Conclusion

Cyber defense must learn from SDI. Cyber defense should have a funded research program with the results from the research being shared between military and commercial organizations. SDI had breakthroughs with particle accelerators and technology related to space exploration. Cyber defense research could have breakthroughs in artificial

[387] David S.F. Portree, "Strategic Defense: Military Uses of the Moon & Asteroids (1983)," *Wired*, February 22, 2015, accessed December 30, 2017, https://www.wired.com/2015/02/strategic-defense-military-uses-moon-asteroid-resources-1983/.

[388] Cooper and Abrahamson, "The Dividends of SDI," 8.

intelligence, blockchain, quantum computing, and/or other emerging technology.[389] An SDI-like cyber research initiative will ensure the continued strengthening of United States cyber defense and provide decades of positive dividends for military and commercial organizations.

[389] Sachchidanand Singh and Nirmala Singh, "Blockchain: Future of Financial and Cyber Security," (paper presented at 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), December 14-17, 2016), accessed January 6, 2018, doi: 10.1109/IC3I.2016.7918009; Amaan Anwar and Syed Imtiyaz Hassan, "Applying Artificial Intelligence Techniques to Prevent Cyber Assaults," *International Journal of Computational Intelligence Research* 13, no. 5 (2017): 883-889, accessed January 6, 2018, http://www.ripublication.com/ijcir17/ijcirv13n5_19.pdf; Aleksandrs Belovs, Gilles Brassard, Peter Hoyer, Marc Kaplan, Sophie Laplante, and Louis Salvail, "Provably Secure Key Establishment Against Quantum Adversaries" (paper presented at Proceedings of the 12th Conference on Theory of Quantum Computation, Communications and Cryptography (TQC), Paris, June 2017), accessed January 6, 2018, https://arxiv.org/abs/1108.2316.

CONCLUSION

LESSONS FOR CYBER POLICYMAKERS

Background

> Critical infrastructure keeps our food fresh, our houses warm, our trade flowing, and our citizens productive and safe. The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.
>
> —*2017 United States National Security Strategy*

Cyberspace is the newest domain of warfare.[390] In cyberspace, the attacker has the advantage over the defender.[391] Cyberspace is unique because it "offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests" without requiring a physical presence.[392] The 2017 United States National Security Strategy states that "America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security."[393] However, in 2006, the United States National Security Strategy, the word "cyber" was

---

[390] Christos Athanasiadis and Ali Rizwan, "Cyber as NATO's Newest Operational Domain: The Pathway to Implementation," *Cybersecurity: A Peer-Reviewed Journal* 1, no. 1 (2017): 48, accessed January 26, 2018, http://www.ingentaconnect.com/content/hsp/jcs/2017/00000001/00000001/art00006.

[391] DoD, *The Department of Defense Cyber Strategy,* 10; U.S. Congress, House, Dugan, *Testimony before the House Armed Services Committee*; Lord and Sharp, eds., *"*America's Cyber Future: Security and Prosperity in the Information Age: Volume 1," 28.

[392] Trump, *National Security Strategy of the United States*, 12.

[393] Ibid.

mentioned one time in parentheses.[394] The rapid rise of cyber from not being a part of the National Security Strategy to a determinant of American prosperity and security means that policymakers have little or no experience developing cybersecurity strategies. To develop an effective foundation for the creation of cybersecurity strategy, cyber policymakers must learn from Cold War deterrence theory and application. The Cold War dealt with a new type of warfare, rapidly evolving technology, and an environment dominated by the offense which mirrors the current challenges in cyberspace. Analysis of Cold War deterrence theory identifies specific principles of deterrence and strategy cyber policymakers can apply to cyber defense.

Defining and Categorizing Cyber Deterrence

Cold War deterrence theorists like Schaub, Quackenbush, Morgenthau, Huth, and Russet assert that deterrence necessitates a threat on the part of the defender.[395] The problem with a threat-based deterrence theory in cyberspace is that success requires the defender to communicate the threat to all potential attackers which is not possible. Smoke, George, Brodie, Nye, and Kahn all contend that deterrence does not necessitate a threat, but the defender must still dissuade the potential attacker from initiating action

[394] Bush, *National Security Strategy of the United States*, 44.

[395] Schaub Jr., "Deterrence, Compellence, and Prospect Theory," 24; Quackenbush, "Deterrence theory: where do we stand?," 741; Morgenthau, "The Four Paradoxes of Nuclear Strategy," 24; Huth and Russett, "Testing Deterrence Theory: Rigor Makes a Difference," 469.

through some form of communication.[396] Furthermore, Smoke, George, Payne, and Freedman argue that effective deterrence requires state-specific communication strategies that take into account unique aspects of each potential attacker.[397] Communication of threats, or cost to potential attackers, is not possible in the current cyber operating environment which creates the first of two dilemmas for cyber policymakers.

The first cyber deterrence dilemma facing U.S. cyber policymakers is: how can the United States deter cyberattacks on infrastructure critical to its national security from the range of potential attackers in cyberspace without being able to communicate the threat or cost to potential attackers? The answer is general strongpoint cyber deterrence. General strongpoint cyber deterrence is the implementation of cyber-specific defensive measures that deny non-state actors and state actors, with limited resources, the ability to attack infrastructure critical to national security without requiring any communication from the defender. Kennan argued that strongpoint defense "allowed the United States to choose the most favorable terrain upon which to confront the Soviet Union."[398] Nye further argued that "by chewing up an attacker's resources and time, a potential target disrupts the cost-benefit model that creates an incentive for attack."[399] General strongpoint cyber deterrence takes lessons from Kennan and Nye because it involves a

---

[396] George and Smoke, *Deterrence in American Foreign* Policy, 182; Brodie, "The Anatomy of Deterrence," 179; Nye Jr., "Deterrence and Dissuasion in Cyberspace," 52; Kahn, *On Thermonuclear War*, 285.

[397] Freedman, "Deterrence and the Balance of Power," 201; Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 31; George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, 181.

[398] Gaddis*, Strategies of Containment*, 58.

[399] Ibid.

focused defense on critical infrastructure that creates a high cost for the attacker forcing him to expend more resources than anticipated. General strongpoint cyber deterrence also forces the attacker to move onto an easier target which is favorable digital terrain for the United States. No deterrent can stop all attacks, but general strongpoint cyber deterrence can limit the pool of potential attackers to state actors with enough resources for a prolonged cyberattack. With the pool of potential initiators limited, the state-specific communication strategies championed by Smoke, George, Freedman, and Payne can be used by cyber policymakers for further deterrence against resourced state actors looking to harm critical infrastructure.[400] State actors who are not affected by a general strongpoint cyber deterrence create a second dilemma for cyber policymakers.

The second cyber deterrence dilemma facing U.S. cyber policymakers is: how can the United States further deter state actors who have the resources to circumvent defenses erected for general cyber deterrence from attacking infrastructure critical to national security? The answer is specific cyber strongpoint deterrence. Unlike general cyber strongpoint deterrence, specific cyber strongpoint deterrence strategies must account for communication with potential initiators, potential attacker rationality, the limits of attribution, and the regional and political contexts in which in attack may occur.[401] The

---

[400] Freedman, "Deterrence and the Balance of Power," 201; Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 31; George & Smoke, *Deterrence in American Foreign Policy*, 181.

[401] Freedman, "Deterrence and the Balance of Power," 201; Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 31; Quackenbush, "Deterrence theory: where do we stand?" 749.; George and Smoke, "Deterrence and Foreign Policy," 172; Morgenthau, "The Four Paradoxes of Nuclear Strategy, 34; Nye Jr., "Deterrence and Dissuasion in Cyberspace," 47; Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option,* 154.

definition of specific cyber strongpoint deterrence, which borrows heavily from Keith Payne, is the focused application of elements of national power against a specific actor accounting for: 1) the potential object of his friction; 2) his motivation and goals (expected gain from attacking); 3) his level of determination; 4)his likelihood of attacking; 5) how he makes decisions; 6) the regional political and security context in which the attack will occur; 7) the likelihood of attribution if he attacks.[402] Unique, state-focused strongpoint cyber deterrence can be effective in communicating the costs of a potential attacks to a finite number of actors. Furthermore, using the right mix of elements of national power against potential attackers can prolong the length of time a cyberattack takes which increases the chance of attribution. Concentrating defensive efforts against specific actors also increases the chance of diverting potential initiators away from attacking infrastructure critical to national security.

Cyber policymakers must implement general and specific strongpoint cyber defense to effectively defend critical infrastructure from cyberattacks. Data is the critical infrastructure in cyberspace which means cyber policymakers must account for the protection of data to create effective general cyber deterrence policies that can enable specific cyber strongpoint deterrence. Encryption, decentralization, and concealment are three principles that require application to data critical to national security for effective general cyber strongpoint deterrence.

[402] Payne, *The Fallacies of Cold War Deterrence and a New Direction*, 102.

Encryption

Herman Kahn recognized that shelter is an important component of protecting infrastructure critical to national security.[403] Kahn argued that "shelter tends to be a good deal more stable than quick reaction alone as a defense" and that "the number of ways in which it can fail seem relatively low."[404] Finally, shelter is part of a broader defense strategy for SNF that also includes mobility, concealment, and dispersion. By itself, shelter is not a complete deterrent, but when combined with mobility, concealment, and dispersion it creates uncertainty for the enemy regarding the location and disposition of SNF. Shelter for nuclear forces parallels encryption in cyberspace where data critical to national security requires protection and hardening from direct enemy attacks. Encryption means "to cipher or encode" which helps protect data from brute-force enemy attacks.[405] Encryption must be used to protect SCADA systems which are currently vulnerable and often unprotected.

Cybersecurity researchers Thomas Marsden, Nour Moustafa, Sitnikova, and Gideon Creech highlight that "research into the security of SCADA systems has grown in recent years, as the potential damage to critical infrastructure including gas, electricity, water, traffic and railway, and/or loss of life and subsequent risk to state security have

---

[403] Kahn, *On Thermonuclear War*, 262.

[404] Ibid.

[405] Simon Singh, *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography* (New York: Anchor Books, 1999), 392.

been realized."[406] Though the risks of attacks to SCADA systems have been identified, "most studies have unveiled that security is an afterthought at best in SCADA systems."[407] Supervisory control systems are vulnerable because they were built on an assumption that "SCADA infrastructure is a closed control ecosystem of sufficiently complex technologies to provide some security through trust and obscurity."[408] Supervisory control systems, like the internet, do not operate in a closed system and are thus vulnerable to cyberattacks from malicious actors. Not only are legacy SCADA systems (e.g. power grid) vulnerable to attack, but future supervisory control systems involving transmitting data through lasers are also neglecting cybersecurity during research and development.

At the Sixteenth International Conference on Accelerator and Large Experimental Control Systems, a team of sixteen scientists and cybersecurity experts led by Leonce Mekinda presented a paper in which they argued that "cybersecurity aspects are often not thoroughly addressed in the design of light source" SCADA systems which

[406] Thomas Marsden, Nour Moustafa, Elena Sitnikova, and Gideon Creech, "Probability Risk Identification Based Intrusion Detection System for SCADA Systems," 1, accessed February 19, 2018, https://arxiv.org/ftp/arxiv/papers/1711/1711.02826.pdf.

[407] Ibid.

[408] Leonce Mekinda, Valerii Bondar, Sandor Brockhauser, Cyril Danilevski, Wajid Ehsan, Sergey Esenov, Hans Fangohr, Gero Flucke, Gabriele Giovanetti, Steffen Hauf, David Gareth Hickin, Anna Klimovskaia, Luis Maia, Thomas Michelat, Astrid Muennich, Andrea Parenti, Hugo Santos, Kerstin Weger, and Chen Xu, "Securing Light Source SCADA Systems" (paper presented at 16th International Conf. on Accelerator and Large Experimental Control Systems, October 8-13, 2017), 1142, accessed February 19, 2018, http://icalepcs2017.vrws.de/papers/thbpa02.pdf.

are currently built on "vulnerable off-the-shelf software."[409] The most high profile light source supervisory control system is the European X-Ray Free Electron Laser contained in a "1.4 billion-euro facility" that produces 15 TB of data each beam."[410] The European X-Ray Free Electron Laser represents the future of SCADA systems and there should be "special care regarding its security."[411] The thread that connects legacy and future supervisory control systems is the lack of effective encryption. If malicious actors can remotely access U.S. SCADA infrastructure, then the threat of a cyberattack against infrastructure to national security will remain high. If encryption can be implemented that forces actors to devote more time and resources to access the data in cyber systems in the form of a general deterrent, then it affords the U.S. more time to implement specific cyber strongpoint deterrence.

In a 2004 report conducted by the Congressional Research Service, Dana Shea made it clear that:

> Encrypting the information transmitted between remote units and their controllers would inhibit inclusion of false information to and from industrial control systems. Current encryption technology may not be compatible due to the time required to process the encrypted data and the level of technology built into control system components. Industrial control systems have stringent timing requirements and tend to be built out of less computationally robust components, which complicate the use of current encryption technologies. While a prototype encryption method for industrial control systems has been developed, it is still in the validation process and is only recently being evaluated for implementation in industry. Further research into encryption techniques for these processes could

[409] Mekinda et al., "Securing Light Source SCADA Systems," 1142.

[410] Ibid.

[411] Ibid.

> provide efficient, market-driven technology for securing industrial control systems information.[412]

Policymakers must learn from Shea's suggestions of investing in the research of encryption techniques to secure SCADA systems.[413] Shea recognized that the injection of false information into SCADA systems could be a major problem and that current encryption technologies might not be able to control the flow of information in SCADA systems.[414] Shea's suggestions in 2004 are just as relevant in 2018 where SCADA systems are susceptible to enemy attacks because of ineffective encryption.[415] Encryption is not a single solution to protecting SCADA systems, but it should be the first step in a general strongpoint cyber deterrence to create a cost that is beyond the resources of nonstate actors and even some state actors. Policymakers cannot forget the importance of encryption when developing policy for infrastructure critical to national cybersecurity because data in SCADA systems requires protection.[416] After the protecting data with encryption, policymakers must understand, as Kahn cautions, that shelter is weakest when the enemy can overwhelm it with an attack that is "larger than the shelters were

---

[412] Dana A. Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat* Congressional Research Service Report for Congress (Washington, DC: Library of Congress, February 2003), 17, accessed February 19, 2018, https://fas.org/irp/crs/RL31534.pdf.

[413] Ibid.

[414] Ibid.

[415] Marsden et al., "Probability Risk Identification Based Intrusion Detection System for SCADA Systems," 2.

[416] Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, 17.

built for."[417] Encryption, like shelter, can also be overwhelmed by overpowering enemy resources in the form of a brute-force attack which means it must not be located in a single place for the enemy to concentrate its resources.[418]

Decentralization

Herman Kahn argued that "one way to prevent the attacker from mounting too large an attack is to disperse shelters to many distinct target points. This forces downward the number of missiles the enemy can shoot at each point."[419] Lawrence Freedman argued that "mobility and concealment" would "discourage an arms race."[420] The 1958 report, *National Policy Implications of Atomic Parity*, also said the "numbers of missiles will avail the enemy nothing, if he does not know the location of the target. We in effect take an initiative which he can overcome only by maintaining hour-to-hour fire-comb surveillance of all our land areas and vast oceans [for SNF]."[421] The principles of mobility directly applies to SCADA systems in cyberspace where "today's centralized information infrastructure is not resistant (to faults or cyber-attacks), extensible or

---

[417] Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, 17.

[418] Bruce Schneier, *Applied Cryptography* (New York: John Wiley & Sons, 1996), 8.

[419] Kahn, *On Thermonuclear War*, 263.

[420] Ibid.; Freedman, *The Evolution of Nuclear Strategy*, 167.

[421] The quotation is from an unclassified summary of *National Policy Implications of Atomic Parity* (Naval Warfare Group Study, Number 5, 1958) and a speech by Admiral Burke to the Press Club on 17 January 1958) contained in Lawrence Freedman, *The Evolution of Nuclear Strategy*, 167.

scalable to accommodate the emerging power grid requirements."[422] In particular, the United States "power grid is deployed with a largely centralized information infrastructure, with the Energy Management System (EMS) acting as the main control center."[423] Cyber policymakers must understand how decentralization applies to cybersecurity strategy to protect infrastructure critical to national security from malicious enemy attacks.

Network decentralization "describes the use of distributed systems and the externalization of software system components."[424] Decentralized networks are the foundation of the cloud which "describes a network-based computer system, which can be used for organizational and technological integration into decentralized information systems, based on cloud computing technology."[425] Florian Kelbert, a research engineer that specializes in information security and privacy, and software engineer Alexander Pretschner argue that "due to the ever-increasing value of data, the continuous protection of sensitive data throughout its entire lifetime has drawn much attention" and that a "decentralized infrastructure overcomes many problems omnipresent in a centralized

---

[422] Young-Jin Kim, Marina Thottan, Vladimir Kolesnikov, and Wonsuck Lee, "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid," *IEEE Communications Magazine* (November 2010*)*: 58, accessed February 29, 2018, https://pdfs.semanticscholar.org/9480/60f857bf4363c2e388ab0b1d1740c42b799c.pdf.

[423] Ibid., 59.

[424] André Müller, André Ludwig, and Bogdan Franczyk, "Data security in decentralized cloud systems – system comparison, requirements analysis and organizational levels," *Journal of Cloud Computing: Advances, Systems and Applications* 6, no. 15 (2017): 2, accessed September 5, 2017, doi: 10.1186/s13677-017-0082-3.

[425] Ibid.

approach."[426] Kelbert and Pretschner also argue that decentralized networks are superior to the current centralized structure because "deploying all components locally and by replicating data to different locations, there is no single point of failure and no need for a central component to be always available for all clients."[427] Furthermore, Kelbert and Pretschner contend that while a solution to data security "could naively be implemented in a centralized fashion, such a solution imposes drawbacks such as being a single point of failure. Intuitively, a centralized solution is also expected to impose significant performance and network communication overhead."[428] Decentralization of data that controls and resides within infrastructure critical to national security must be a tenet of any cybersecurity deterrence strategy to add an additional layer of complexity to encrypted data and create uncertainty for the attacker.

Young-Jin Kim, Marina Thottan, Vladimir Kolesinkov, and Wonsuck Lee, a group of experts ranging from electrical engineering to cryptography, argue that "important differentiator for the next generation power grid is the massive amounts of measurement data that will be made available at distributed locations that can and must be leveraged optimally to operate the power grid."[429] The arguments of Kim, Thottan,

---

[426] Florian Kelbert and Alexander Pretschner, "A Fully Decentralized Data Usage Control Enforcement Infrastructure" (paper presented at the proceedings of the 13th International Conference on Applied Cryptography and Network Security, June 2015), 1 and 18, accessed February 17, 2018, https://www.doc.ic.ac.uk/~fkelbert/papers/acns15.pdf.

[427] Ibid.

[428] Ibid., 410.

[429] Kim et al., "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid," 59.

Kolesinkov, Lee, Kelbert, and Pretschner, are the cyber equivalent to arguments for decentralization made by Brodie, Kahn, Freedman, and the Naval Warfare Group.[430] Cybersecurity policymakers must incorporate decentralization into their general and specific deterrence strategies because it creates uncertainty as to the location of data that is critical to national security. When the defender can ensure that data critical to national security is never centralized and constantly moving, it means the attacker never has the opportunity to mass his offensive capabilities against one particular location. Decentralized data also makes encryption even more important because it adds a layer of security that increases the cost for the attacker. Not only does the attacker need to find the location(s) of data critical to national security, but he also has to defeat the defender's encryption at each location that contains portions of the data. Cyber policymakers that understand the necessity of data centralization can shape an environment that is advantageous for the defender. Cyber policymakers must also understand how to augment the effects of encryption and decentralization by concealing the whereabouts and type of encryption of data critical to national security.

Concealment

Bernard Brodie, Herman Kahn, Martin Van Creveld and Lawrence Freedman championed concealment for SNF.[431] Brodie argued that concealed SNF (along with

---

[430] Brodie, "Implications for Military Policy," 76, 88-91; Kahn, *On Thermonuclear War*, 264; Freedman, *The Evolution of Nuclear Strategy*, 167.

[431] Brodie, "The Anatomy of Deterrence," 181; Kahn, *On Thermonuclear War*, 263-264; Van Creveld, *The Transformation of War*, 9; Freedman, *The Evolution of Nuclear Strategy*, 167.

sheltered and dispersed) made it more likely that SNF would survive a first strike and less likely that the attacker would surprise the defender.[432] Kahn thought that concealment by "continuous mobility or reasonably frequent changes of position" challenged the enemy's intelligence and created confusion and force them to expend resources creating a larger attacking force.[433] Van Creveld highlighted multiple courses of action considered by the United States for concealment of SNF to include subterranean tunnels with tracks, missiles that were dug thousands of feet deep that would be launched from underground after surviving an attack, and platforms that would "crawl over the bottom of the lakes."[434] Freedman thought concealment (and mobility) "discourage[d] an arms race" because "numbers of missiles will avail the enemy nothing, if he does not know the location of his target."[435] Analysis of concealment by Brodie, Kahn, Van Creveld, and Freedman directly applies to cyberspace because "infrastructure that causes the greatest concern in the cyber war literature, industrial control systems, can also be protected by deception."[436]

Even with a general cyber deterrent in place, "We must assume, then, that an adversary will breach border controls and establish footholds within the defender's

---

[432] Brodie, "The Anatomy of Deterrence," 181.

[433] Kahn, *On Thermonuclear War*, 263-264

[434] Van Creveld, The Transformation of War, 9

[435] Freedman, *The Evolution of Nuclear Strategy*, 167.

[436] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 341, accessed February 19, 2018, doi: 10.1080/09636412.2015.1038188.

network, so we need to study and engage the adversary on the defender's turf in order to influence any future moves."[437] Dr. Kristin E. Heckman, lead scientist at The MITRE Corporation in McLean, VA and a team of MITRE scientists argued that a key component in an environment in which an attacker will enter the defender's network even with the most elaborate security measures, "is cyber denial and deception."[438] Furthermore, Heckman and her team said:

> The goal of D&D is to influence another to behave in a way that gives the deceiver an advantage, creating a causal relationship between psychological state and physical behavior. Denial actively prevents the target from perceiving information and stimuli; deception provides misleading information and stimuli to actively create and reinforce the target's perceptions, cognitions, and beliefs. Both methods generate a mistaken certainty in the target's mind about what I s and is not real, making the target erroneously confident and ready to act.[439]

Heckman and the scientists at MITRE made it clear that adding a layer of deception in the form of concealing information for which the attacker is searching adds another layer of complexity to deterrence by denial.[440] Political scientists Erik Gartzke and Jon R. Lindsay further discuss deception in the cyber domain and claim that "deception is logically different from denial even though they are often combined. Pure defense is the act of physically confronting attackers so that they cannot cause harm to the assets that are being defended. Deception, by contrast, conceals assets and pitfalls from the

---

[437] Kristin E. Heckman, Frank J. Stech, Ben S. Schmoker, and Roshan K. Thomas, "Denial and Deception in Cyber Defense," *Computer* 48, no. 4 (2015): 32, doi: 10.1109/MC.2015.

[438] Ibid.

[439] Ibid.

[440] Ibid.

enemy."[441] Gartzke and Lindsay further argue that "cyberspace heightens the effectiveness of deception" and highlight that "an adversary that wanted to complain about defensive deception would also have first to revel its identity."[442]

In an experiment involving cyber deception, Gartzke and Lindsay found "in one real-time red-team versus blue-team cyber war game experiment, a honeypot[443] system failed to deny red-team hackers access to the command and control mission system, but decoys and disinformation did succeed in preventing the adversary from obtaining sensitive data."[444] Heckman and a team of scientists from MITRE also found that "traditional denial and deception techniques were effective in denying the adversary access to real information on the real command and control mission system, and instead provided the adversary with access to false information on a fake command and control mission system."[445]

---

[441] Gartzke and Lindsay, Weaving Tangled Webs," 337.

[442] Ibid., 338 and 339.

[443] A honeypot is a program, machine, or system put on a network as bait for attackers. The idea is to deceive the attacker by making the honeypot seem like a legitimate system. A honeynet is a network of honeypots set up to imitate a real network. Honeynets can be configured in both production and research environments. A research honeynet studies the tactics and methods of attackers. This definition was retrieved from the SANS Institute at https://www.sans.org/reading-room/whitepapers/detection/hands-honeypot-365.

[444] Ibid., 341.

[445] Kristin E. Heckman, Michael J.Walsh, Frank J.Stech, Todd A.O'Boyle, Stephen R.DiCato, "Active cyber defense with denial and deception: A cyber-wargame experiment," *Computers and Security* 37 (September 2013): 72, accessed February 10. 2018, doi: 10.1016/j.cose.2013.03.015.

Gartzke, Lindsay, Heckman and MITRE scientists, make it clear that deception will have a major impact on a defender's ability to deter in cyberspace.[446] Jeffrey Pawlick, U.S. Army Research Laboratory, Edward Colbert, U.S. Army Research Laboratory, and Quanyan Zhu, New York University Tandon School of Engineering, further researched cyber deception and developed a taxonomy that defined six types of deception: "perturbation, moving target defense, obfuscation, mixing, honey-x, and attacker-engagement."[447] Pawlick, Colbert, and Zhu's analysis does not argue that any one type of deception is the best in cyberspace, but rather breaks methods of concealing information through deception down into different categories.[448] Cyber deception can augment general strongpoint cyber deterrence by further concealing information even if an attacker makes it through a cyber defense. Concealment of information can drive up the cost, time, and complexity for the attacker, create more time for the defender to attribute an attack, and filter out more potential attackers. Cyber policymakers must understand how to incorporate concealment in conjunction with encryption and decentralization into a general strongpoint cyber deterrent to create a layered approach that limits the number of potential attackers and affords the United States an opportunity

[446] Heckman et al., "Active cyber defense with denial and deception: A cyber-wargame experiment," 72; Heckman et al., "Denial and Deception in Cyber Defense," 32.

[447] Jeffrey Pawlick, Edward Colbert, and Quanyuan Zhu, "A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy," Submitted for review to ACM Computing Surveys, 1, accessed January 18, 2018. https://arxiv.org/abs/1712.05441.

[448] Ibid.

to implement a specific strongpoint cyber deterrence against a manageable number of initiators.

Conclusion

Cybersecurity deterrence requires a forward-thinking approach and not a reliance on specific solutions. Analysis of Cold War deterrence theory results in the following lessons from which cybersecurity policymakers must learn and incorporate to develop a forward-thinking approach to defending critical infrastructure in cyberspace:

1. The initial layer of cyber deterrence must be focused on denying potential attackers because it is not possible to communicate with all potential initiators.
2. Threat-based deterrence is not possible in cyberspace unless the range of potential attackers is greatly reduced.
3. Cyber deterrence must be focused on strongpoints because a perimeter defense will be costly for the defender, and not effective against potential initiators. Strongpoints in cyberspace are infrastructure critical to national security.
4. Critical infrastructure in cyberspace should be encrypted, decentralized, and concealed to increase the cost for the attacker, buy time for the defender, and increase the chance of attribution of the attacker.
5. Resources must be allocated to researching emerging and future capabilities to create innovation opportunities for long-term cyber defense.
6. A technology-focused general strongpoint cyber deterrent creates the opportunity for an actor-specific specific strongpoint cyber deterrence strategy

that leverages the elements of national bower beyond just cyber defense technology.

7. Specific strongpoint cyber deterrence that leverages the elements of national power and actor-specific considerations can be used following the employment of a general strongpoint cyber deterrent to target a limited number of potential initiators with the resources to target U.S. infrastructure critical to national security.

The long-term approach to cyber defense must use a framework with the lessons identified from Cold War deterrence theory and implementation. A framework is a set of adaptable principles that can be applied to evolving problem-sets. Cybersecurity is an evolving problem-set that must have adaptable policymakers capable of simultaneously addressing current and long-term threats through the implementation of general and specific strongpoint cyber deterrence. General and strongpoint cyber deterrence that leverages the lessons identified during the Cold War and applies them to cyberspace will have a foundation on which they can build iterative cyber defenses that continually incorporate new technology to address evolving threats.

BIBLIOGRAPHY

Books

Belous, Vladimir, *Shield of Russia: Systems of Missile Defense*. Moscow: Publishing House of N.E. Bauman Moscow Technical State University, 2009.

Bethe, Hans A. "Countermeasures to ABM Systems. "In *ABM: An Evaluation of the Decision to Deploy an Antiballistic Missile System*, edited by Abram Chayes and Jerome B. Wiesner (New York: Harper & Row, 1969), 142

Bowman, Robert. *Star Wars: Defense or Death Star?* Bethesda, MD: Institute for Space and Security Studies, 1985.

Brodie, Bernard. "Implications for Military Policy." In *The Absolute Weapon: Atomic Power and World Order,* edited by Bernard Brodie, 57-89. New York: Harcourt, Brace, and Company, 1946.

———. *Strategy in the Missile Age*. Princeton, NJ: Princeton University Press, 1959.

Chayes, Abram, and Jerome B. Wiesner, eds. *ABM: An Evaluation of the Decision to Deploy an Antiballistic Missile System*. New York: Harper & Row, 1969.

Doughtery, James E. and Robert L. Pfaltzgraff. *Contending Theories of International Relations: A Comprehensive Survey*. New York: Longman, 2001.

Fitzgerald, Frances. *Way Out There in the Blue: Reagan, Star Wars, and the End of the Cold War*. New York: Simon and Schuster, 2000.

Freedman, Lawrence. *The Evolution of Nuclear Strategy*. New York: St. Martin's Press, 1981.

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

Gaddis, John Lewis. *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War*. New York: Oxford University Press, 2005.

George, Alexander, and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press, 1974.

Gruntman, Mike. *Intercept 1961: The Birth of Soviet Missile Defense*. Reston, VA: American Institute of Aeronautics and Astronautics, 2015.

Hobbes, Thomas. *Leviathan*. New York: Penguin Books, 1968.

Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Lanham, MD: Rowman and Littlefield, 2017.

Jones, Frank. “The Strategic Dimensions of Terrorism: Concepts, Countermeasures, and Conditions in Search for Security.” In *Influence Warfare: How Terrorist and Governments Fight to Shape Perceptions in a War of Ideas*, edited by J. J. Forest, 123-151. Westport, CT: Praeger Security International, 2009.

Kagan, Donald. *On the Origins of War and the Preservation of Peace*. New York: Doubleday, 1995.

Kahn, Herman. *On Thermonuclear War*. Princeton, NJ: Princeton University Press, 1960.

Kalic, Sean N. “Europe and Reagan’s SDI Announcement.” In *the Crisis of Détente in Europe: From Helsinki to Gorbachev*, edited by Leopoldo Nuti, 99-110. New York: Routledge, 2009.

Kennan, George F. *Russia, the Atom, and the West*. New York, Harper & Brothers, 1958.

Krepenivich, Andrew. *Cyberwarfare: A Nuclear Option?* Washington, DC: Center for Strategic and Budgetary Assessments. Accessed August 27, 2017. http://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option/publication.

Miller, S. E., and S. Van Evera, eds. *The Star Wars Controversy*. Princeton, NJ: Princeton University Press, 1986.

Mills, David W. *Cold War in a Cold Land: Fighting Communism on the Northern Planes*. Norman: University of Oklahoma Press, 2015.

Naim, Moises. *The End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge Isn’t What it Used to Be*. New York: Basic Books, 2013.

Napoleoni, Loretta. *North Korea: The Country We Love to Hate*. Crawley, Australia: UWA Publishing, 2018.

Payne, Keith *The Fallacies of Cold War Deterrence and a New Direction*. Lexington: The University Press of Kentucky, 2001.

Prados, John. “The Strategic Defense Initiative: Between Strategy, Diplomacy and US Intelligence Estimates.” In *the Crisis of Détente in Europe: From Helsinki to Gorbachev*, edited by Leopoldo Nuti, 86-98. New York: Routledge, 2009.

Reagan, Ronald. *An American Life*. New York: Simon and Schuster, 1990.

Rodberg, Leonard S. “ABM Reliability.” In *ABM: An Evaluation of the Decision to Deploy an Antiballistic Missile System*, edited by Abram Chayes and Jerome B. Wiesner, 107-117. New York: Harper & Row, 1969.

Schneier, Bruce. *Applied Cryptography*. New York: John Wiley & Sons, 1996.

Singh, Simon. *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography*. New York: Anchor Books, 1999.

Stein, Janet Gross. "Rational Deterrence against Irrational Adversaries." In *Complex Deterrence: Strategy in the Global Age,* edited by. T. V. Paul, Patrick M. Morgan, and James J. Wirtz, 58-84. Chicago, IL: University of Chicago Press, 2009.

Van Creveld, Martin. *The Transformation of War*. New York: The Free Press, 1991.

Waltz, Kenneth. *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press, 1959.

Yarger, Harry R. "Toward a Theory of Strategy." In *Guide to National Security Policy and Strategy*, 2nd ed., 107-113. Carlisle, PA: United States Army War College, 2006.

Periodicals

Anwar, Amaan, and Syed Hassan Imtiyaz. "Applying Artificial Intelligence Techniques to Prevent Cyber Assaults." *International Journal of Computational Intelligence Research* 13, no. 5 (2017): 883-889. Accessed January 6, 2018. http://www.ripublication.com/ijcir17/ijcirv13n5_19.pdf.

Athanasiadis, Christos, and Ali Rizwan. "Cyber as NATO's Newest Operational Domain: The Pathway to Implementation." *Cybersecurity: A Peer-Reviewed Journal* 1, no. 1 (2017): 48-60. Accessed January 26, 2018. http://www.ingentaconnect.com/content/hsp/jcs/2017/00000001/00000001/art00006.

Bartosz, Jasiul, Marcin Szpyrka, and Joanna Sliwa. "Detection and Modeling of Cyber Attacks with Petri Nets." *Entropy* 16, no. 12 (2014): 6602-6623. Accessed January 6, 2018. doi:10.3390/e16126602.

Brantly, Aaron. "The Most Governed Ungoverned Space: Legal and Policy Constraints on Military Operations in Cyberspace." *Johns Hopkins SAIS Review* 36, no. 2 (2016): 29-39. Accessed September 9, 2017. https://muse.jhu.edu/article/641158.

Brodie, Bernard. "The Anatomy of Deterrence." *World Politics* 11, no. 2 (1959): 173-191. Accessed August 27, 2017. https://www.jstor.org/stable/2009527.

Cooper, Henry F. and James A. Abrahamson. "The Dividends of SDI." *The Journal of International Security Affairs Symposium: Modern Missile Defense at 30* (2013): 7-9. Accessed December 30, 2017. http://highfrontier.org/wp-content/uploads/2013/06/The-Dividends-of-SDI.pdf.

Freedman, Lawrence. “Beyond Surprise Attack.” *Parameters* 47, no. 2 (2017): 7-13. Accessed November 25, 2017. http://ssi.armywarcollege.edu/pubs/Parameters/issues/Summer_2017/4_Freedman_BeyondSurpriseAttack.pdf.

———. “General Deterrence and the Balance of Power.” *Review of International Studies* 15, no. 2 (1989): 199-210. Accessed August 25, 2017. https://www.jstor.org/stable/20097179.

Gartzke, Erik, and Jon R. Lindsay. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies* 24, no. 2 (2015): 316-348. Accessed February 19, 2018. doi: 10.1080/09636412.2015.1038188.

George, Alexander L., and Smoke, Richard. “Deterrence and Foreign Policy.” *World Politics* 41, no. 2 (1989): 170-182. Accessed August 25, 2017. https://www.jstor.org/stable/2010406?seq=1#page_scan_tab_contents.

Goldman, Zachary, and Damon McCoy. “Deterring Financially Motivated Cybercrime.” *Journal of National Security Law & Policy* 8, no. 3 (2016): 1-22. Accessed August 28, 2017. http://jnslp.com/wpcontent/uploads/2016/07/Deterring_Financially_Motivated_Cybercrime.pdf.

Heckman, Kristin E., Frank J. Stech, Ben S. Schmoker, and Roshan K. Thomas. “Denial and Deception in Cyber Defense.” *Computer* 48, no. 4 (2015): 32-40. Accessed January 26, 2018. doi: 10.1109/MC.2015.

Heckman, Kristin E., Michael J. Walsh, Frank J. Stech, Todd A. O’Boyle, and Stephen R. DiCato. “Active cyber defense with denial and deception: A cyber-wargame experiment.” *Computers and Security* 37 (September 2013): 72-77. Accessed February 10, 2018. doi: 10.1016/j.cose.2013.03.015.

Hjortdal, Magnus. “China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence.” *Journal of Strategic Security* 4, no. 2 (2011): 1-24. Accessed February 10, 2018. doi: http://dx.doi.org/10.5038/1944-0472.4.2.1

Huth, Paul, and Bruce Russett. “Testing Deterrence Theory: Rigor Makes a Difference.” *World Politics* 42, no. 4 (1990): 466-501. Accessed August 25, 2017. https://www.jstor.org/stable/2010511?seq=1#page_scan_tab_contents.

Iasiello, Emilio. “Hacking Back: Not the Right Solution.” *Parameters* 44, no. 3 (2014): 105-113. Accessed September 5, 2017. http://ssi.armywarcollege.edu/pubs/parameters/issues/Autumn_2014/13_IasielloEmilio_Hacking%20Back%20Not%20the%20Right%20Solution.pdf.

———. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7, no. 1 (2013): 54-67. Accessed October 29, 2017. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1337&context=jss.

Kim, Young-Jin, Marina Thottan, Vladimir Kolesnikov, and Wonsuck Lee. "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid." *IEEE Communications Magazine* (November 2010): 58-62. Accessed February 29, 2018. https://pdfs.semanticscholar.org/9480/60f857bf4363c2e388ab0b1d1740c42b799c.pdf.

Klein, John. "Deterring and Dissuading Cyberterrorism." *Journal of Strategic Security* 8, no. 4 (2015): 23-38. Accessed September 5, 2017. doi: http://dx.doi.org/10.5038/1944-0472.8.4.1460.

Müller, André, André Ludwig, and Bogdan Franczyk. "Data security in decentralized cloud systems – system comparison, requirements analysis and organizational levels." *Journal of Cloud Computing: Advances, Systems and Applications* 6, no. 15 (2017): 1-9. Accessed September 5, 2017. doi: 10.1186/s13677-017-0082-3.

Levy, Jack S. "Deterrence and Coercive Diplomacy: The Contributions of Alexander George." *Political Psychology* 29, no. 4 (2008): 537-552. Accessed August 25, 2017. https://www.jstor.org/stable/20447143.

Morgenthau, Hans J. "The Four Paradoxes of Nuclear Strategy." *The American Political Science Review* 58, no. 1 (1964): 23-35. Accessed August 31, 2017. https://www.jstor.org/stable/1952752.

Nye Jr., Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2017): 44-71. Accessed September 26, 2017. doi: 10.1162/ISEC_a_00266.

Palmer, Miles, and Roger Lenard. "A Revolution in Access to Space Through Spinoffs of SDI Technology." *IEEE Transactions on Magnetics* 27, no. 1 (1991): 11-20. Accessed December 30, 2017. http://ieeexplore.ieee.org/document/100986/.

Pfaff, C. Anthony. "Five Myths about Military Ethics." *Parameters* 46, no. 3 (2016): 59-69. Accessed September 13, 2017. https://ssi.armywarcollege.edu/pubs/parameters/issues/Autumn_2016/9_Pfaff.pdf.

Rid, Thomas. "Cyber War Will Not Take Place." *The Journal of Strategic Studies* 35, no. 1 (2011): 5-32. Accessed October 29, 2017. doi: 10.1080/01402390.2011.608939.

Schaub Jr., Gary. "Deterrence, Compellence, and Prospect Theory." *Political Psychology* 25, no. 3 (2004): 389-411. Accessed August 25, 2017. https://www.jstor.org/stable/3792549.

Tor, Uri. "Cumulative Deterrence as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40, no. 1 (2017), 92-117. Accessed September 5, 2017. doi:10.1080/0140202390.2015.1115975.

Quackenbush, Stephen. "Deterrence theory: where do we stand?" *Review of International Studies* 37, no. 2 (2011): 741-762. Accessed August 25, 2017. https://www.jstor.org/stable/23024618.

Conference Papers

Applegate, Scott D. "The Principle of Maneuver in Cyber Operations." Paper presented at Cyber Conflict (CYCON), 2012 4th International Conference on Cyber Conflict, Estonia, June 5-7, 2012. Accessed December 1, 2017. http://ieeexplore.ieee.org/document/6243974/.

Belovs, Aleksandrs, Gilles Brassard, Peter Hoyer, Marc Kaplan, Sophie Laplante, and Louis Salvail. "Provably Secure Key Establishment Against Quantum Adversaries." Paper presented at Proceedings of the 12th Conference on Theory of Quantum Computation, Communications and Cryptography (TQC), Paris, June 2017. Accessed January 6, 2018. https://arxiv.org/abs/1108.2316.

Benton, J., Robert P. Goldman, Mark Burstein, Joseph Mueller, Paul Robertson, Dan Cerys, Andreas Hoffman, and Rusty Bobrow. "Active Perception for Cyber Intrusion Detection and Defense." Paper presented at The Workshops of the Thirtieth AAAI Conference on Artificial Intelligence Artificial Intelligence for Cyber Security: Technical Report WS-16-03, Cambridge, MA, September 21-25, 2013. Accessed November 26, 2017. doi: 10.1109/SASOW.2015.20.

Kelbert, Florian, and Alexander Pretschner. "A Fully Decentralized Data Usage Control Enforcement Infrastructure." Paper presented at proceedings of the 13th International Conference on Applied Cryptography and Network Security, June 2015. Accessed January 6, 2018. https://www.doc.ic.ac.uk/~fkelbert/papers/acns15.pdf.

Lu, Xun, Jianwei Zhuge, Ruoyu Wan, Yinzhi Cao, and Yan Chen. "De-Obfuscation and Detection of Malicious PDF Files with High Accuracy." Paper presented at the 46th Hawaii International Conference on System Sciences, 7-10 January 2013. Accessed January 6, 2018. https://doi.org/10.1109/HICSS.2013.166.

Mekinda, Leonce, Valerii Bondar, Sandor Brockhauser, Cyril Danilevski, Wajid Ehsan, Sergey Esenov, Hans Fangohr, Gero Flucke, Gabriele Giovanetti, Steffen Hauf, David Gareth Hickin, Anna Klimovskaia, Luis Maia, Thomas Michelat, Astrid Muennich, Andrea Parenti, Hugo Santos, Kerstin Weger, and Chen Xu. "Securing Light Source SCADA Systems." Paper presented at 16th International Conference on Accelerator and Large Experimental Control Systems, October 8-13, 2017. Accessed February 19, 2018. http://icalepcs2017.vrws.de/papers/thbpa02.pdf.

Montanarelli, Nick, and Ted Lynch. "Applications of the Strategic Defense Initiative's Compact Accelerators." Paper presented at NASA, Washington, Technology 2001: The Second National Technology Transfer Conference and Exposition Vol. 2. Accessed December 30, 2017. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19920013489.pdf.

Romero-Mariona Jose, Megan Kline, and John San Miguel. "C-SEC (Cyber SCADA evaluation capability): Securing critical infrastructures." Paper presented at 2015 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Gaithersburg, MD, November 2-5, 2017. Accessed February 19, 2018. http://ieeexplore.ieee.org/abstract/document/7392035/.

Sheperd, Daniel P., Todd E. Humphreys, and Aaron A. Fansler. "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks." Paper presented at Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Washington, DC, March 19-21, 2012. Accessed September 16, 2017. https://radionavlab.ae.utexas.edu/images/stories/files/papers/spoofSMUCIP2012.pdf.

Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of Financial and Cyber Security." Paper presented at 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), December 14-17, 2016. Accessed January 6, 2018. doi: 10.1109/IC3I.2016.7918009.

Venkatesan, Sridhar, Massimiliano Albanese, George Cybenko, and Sushil Jajodia, "A Moving Target Defense Approach to Disrupting Stealth Botnets." Paper presented at Proceedings of the 2016 ACM Workshop on Moving Target Defense. Accessed December 30, 2017. https://www.researchgate.net/profile/Massimiliano_Albanese/publication/310821206_A_Moving_Target_Defense_Approach_to_Disrupting_Stealthy_Botnets/links/592b3fe9a6fdcc44435b11e6/A-Moving-Target-Defense-Approach-to-Disrupting-Stealthy-Botnets.pdf.

Zheng, Ren, Wenlian Lu, and Shouhuai Xu. "Optimizing Active Cyber Defense." Paper presented at Proceedings of the 4th Conference on Decision and Game Theory for Security, 2016. Accessed November 25, 2017. arXiv:1603.08312 [cs.CR].

Government Documents

Bush, George W. *National Security Strategy of the United States*. Washington, DC: The White House. Accessed December 30, 2017. https://www.state.gov/documents/organization/64884.pdf.

Department of Defense. *The Department of Defense Cyber Strategy*. Washington, DC: Department of Defense, April 2015. Accessed September 1, 2017. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Department of Defense, Defense Science Board. *Task Force on Cyber Deterrence*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017. Accessed August 31, 2017. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

McNamara, Robert. Secretary of Defense. "Mutual Deterrence." San Francisco, September 18, 1967. Accessed January 17, 2018. http://www.atomicarchive.com/Docs/Deterrence/Deterrence.shtml.

Reagan, Ronald. National Security Decision Directive 6-83, *Study on Eliminating the Threat Posed by Ballistic Missiles*. Washington, DC: The White House. Accessed September 17, 2017. https://catalog.archives.gov/id/6858544.

———. National Security Decision Directive 85, *Eliminating the Threat from Ballistic Missiles*. Washington, DC: The White House. Accessed September 17, 2017. https://reaganlibrary.archives.gov/archives/reference/Scanned%20NSDDS/NSDD85.pdf.

———. Speech on 'Defense Spending and Defense Technology,' March 23, 1983. In *Office of Technology Assessment (OTA), Strategic Defenses Ballistic Missile Defense Technologies: Anti-Satellite Weapons, Countermeasures, and Arms Control*, 297-298. Princeton, NJ: Princeton University Press, 1986.

Rogers, Michael. *Statement of Admiral Michael S. Rogers Commander United States Cyber Command*. Washington, DC, May 9, 2017. Accessed September 29, 2017. https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

Trump, Donald. *National Security Strategy of the United States*. Washington, DC: The White House. Accessed December 30, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

U.S. Congress. House. Defense Advanced Research Projects Agency Director Regina E. Dugan. *Testimony before the House Armed Services Committee*, Subcommittee on Emerging Threats and Capabilities. Washington, DC, 1 March 2011. Accessed January 17, 2018. https://www.darpa.mil/attachments/TestimonyArchived%20(March%201%202011).pdf.

U.S. Congress. *Hearings before Subcommittee of Committee on Armed Services*. Washington, DC, 1960.

Other Sources

Center for Cyber and Homeland Security. "Into the Gray Zone: The Private Sector and Active Cyber Defense against Cyber Threats." Project Report, George Washington University Center for Cyber and Homeland Security, Washington, DC, October 2016. Accessed December 2017. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Centre for the Protection of National Infrastructure (CPNI). "Configuring and Managing Remote Access for Industrial Control Systems." Project Report, CPNI, United Kingdom, November 2010. Accessed December 30, 2017. https://scadahacker.com/library/Documents/Best_Practices/DHS%20-%20Remote%20Access%20for%20ICS.pdf.

Center of Military History. "History of Strategic and Ballistic Missile Defense Volume II 1956-1972." Project Report, Center of Military History, Washington, DC, 2009.

Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." Project Report, Center for Naval Analyses, Alexandria, VA, March 2017. Accessed September 1, 2016. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Greenberg, Andy. "Hackers Gain Direct Access to US Power Grid Controls." *Wired.* Accessed September 29, 2017. https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

Idaho National Laboratory (Mission Support Center). "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." Project Report, Idaho National Laboratory, Idaho Falls, ID, August 2010. Accessed February 3, 2018. https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

Kowalski, Eileen, and Dawn Cappelli. "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector." Project Report, National Threat Assessment Center, Washington, DC, January 2008. Accessed December 7, 2017. https://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52266.pdf.

Lewis, Jim. "Cyber Deterrence." Speech presented at Stimson's programming on Space Security, Washington, DC, 2012. Accessed August 26, 2017. https://www.stimson.org/content/jim-lewis-csis-speaks-stimson-cyber-deterrence.

Lord, Kristin M., and Travis Sharp, eds. "America's Cyber Future: Security and Prosperity in the Information Age: Volume 1." Project Report, Center for a New American Security, Washington, DC, June 2011. Accessed November 25, 2017. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238.

Loma Linda University Proton Treatment & Research Center. "What is Proton Therapy?" Accessed December 30, 2017. https://protons.com/.

Manjikian, Mary. "Deterring Cybertrespass and Securing Cyberspace: Lessons From United States Border Control Strategies*."* Project Report, United States Army War College, Strategic Studies Institute, Carlisle, PA, December 2016. Accessed February 13, 2018. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1332.

Marsden, Thomas, Nour Moustafa, Elena Sitnikova, and Gideon Creech. "Probability Risk Identification Based Intrusion Detection System for SCADA Systems." Accessed February 19, 2018. https://arxiv.org/ftp/arxiv/papers/1711/1711.02826.pdf.

McKenzie, Timothy. *Is Cyber Deterrence Possible?* Maxwell AFB, AL: Air University Press, January 2017. Accessed August 27, 2017. http://www.au.af.mil/au/aupress/digital/pdf/paper/cpp_0004_mckenzie_cyber_deterrence.pdf.

Pacific Northwest National Laboratory. "Cyber Deterrence and Stability: Assessing Cyber Weapons Analogous through Existing WMD Deterrence and Arms Control Regimes." Project Report, Pacific Northwest National Laboratory, Alexandria, VA, September 2017. Accessed November 26, 2017. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26932.pdf.

Pawlick, Jeffrey, Edward Colbert, and Quanyuan Zhu. "A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy." Accessed January 18, 2018. https://arxiv.org/abs/1712.05441.

Portree, David S.F. Strategic Defense: "Military Uses of the Moon & Asteroids (1983)." *Wired*, February 22, 2015. Accessed December 30, 2017. https://www.wired.com/2015/02/strategic-defense-military-uses-moon-asteroid-resources-1983/.

Shea, Dana A. *Critical Infrastructure: Control Systems and the Terrorist Threat*. Congressional Research Service Report for Congress. Washington, DC: Library of Congress, February 2003. Accessed February 19, 2018. https://fas.org/irp/crs/RL31534.pdf.

Sokolovsky, Vasilii D. *Soviet Military Strategy.* Accessed September 10, 2017. https://www.rand.org/content/dam/rand/pubs/reports/2005/R416.pdf

Torrence, James. "GPS: Infrastructure and Technical Vulnerabilities." *Small Wars Journal*, February 1, 2017. Accessed September 1, 2017. http://smallwarsjournal.com/jrnl/art/gps-infrastructure-and-technical-vulnerabilities.

van der Meer, Sico, and Francil Paul van der Putten. “US Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations.” Project Report, Netherlands Institute of International Relations, Clingendael, Netherlands, September 2015. Accessed September 10, 2017. https://www.clingendael.org/publication/danger-proliferating-covert-cyber-operations.

van Tol, Jan Mark Gunzinger, Andrew Krepenevich, and Jim Thomas. “AirSea Battle: A Point-of- Departure Operational Concept.” Project Report, Center for Strategic and Budgetary Assessments, Washington, DC, 2010. Accessed November 25, 2017. http://csbaonline.org/research/publications/airsea-battle-concept/publication.

United States Army War College. *Strategic Cyberspace Operations Guide*. Carlisle, PA: U.S. Army War College. Accessed December 7, 2017. https://www.csl.army.mil/usacsl/Publications/Strategic_Cyberspace_Operations_Guide_1_June_2016.pdf.