

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 17-06-2013	2. REPORT TYPE Master's Thesis	3. DATES COVERED (From - To) 23-07-2012 to 14-06-2013
--	--	---

4. TITLE AND SUBTITLE Paradigm Change: Cybersecurity of Critical Infrastructure	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S) LTC James E. Martin, Jr., USAR	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton Blvd Norfolk, VA 23511-1702	8. PERFORMING ORGANIZATION 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
This study argues that the United States paradigm for the cybersecurity of critical infrastructure is flawed. For nearly two decades, repeated Presidential attempts, along with Congressional efforts, to revise cybersecurity policies result in new policies that contain old and unproven principles. Meanwhile, the cyber vulnerabilities within critical infrastructure information environments and the lethality of the global cyber threats to those national assets continue to grow. This research identifies and examines the foundational policy threads that resurface within consecutive Presidential cybersecurity policy initiatives over the previous twenty years. Collectively, these consistent themes constitute the United States' paradigm for cybersecurity. Although the United States' approach to cybersecurity cumulatively evolved during the past twenty years, its foundational principles remain unchanged, in error, and incapable of solving the nation's cybersecurity challenges. Specifically, two unproven beliefs, the Self-Regulation and Incremental Progress theories, remain consistent stalwarts throughout subsequent polices covering the cybersecurity of critical infrastructure` lens of Thomas Kuhn's change theory. Periodically a series of events creates a critical point in which the long-held beliefs cease to resolve the complexities within an environment and create the conditions for a paradigm change. The United States is at just such an inflection point.

15. SUBJECT TERMS
Cybersecurity policy; critical infrastructure; paradigm shift; paradigm change

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unclassified Unlimited	18. NUMBER OF PAGES 87	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (include area code) 757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL



**PARADIGM CHANGE: CYBERSECURITY OF CRITICAL
INFRASTRUCTURE**

by

James Edward Martin, Jr.

Lieutenant Colonel, United States Army Reserve

**PARADIGM CHANGE: CYBERSECURITY OF CRITICAL
INFRASTRUCTURE**

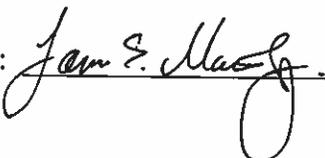
by

James Edward Martin, Jr.

Lieutenant Colonel, United States Army Reserve

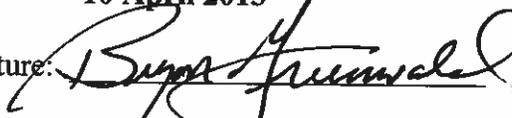
A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature:  _____

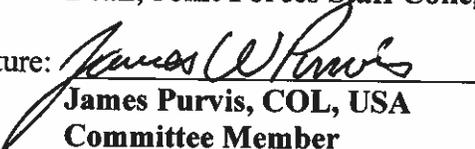
10 April 2013

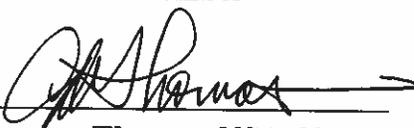
**Thesis Adviser:
Name**

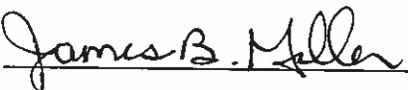
Signature:  _____

**Bryon Greenwald, Ph.D
Dean, Joint Forces Staff College**

Approved by:

Signature:  _____
**James Purvis, COL, USA
Committee Member**

Signature:  _____
**Gregory Thomas, NSA Chair
Committee Member**

Signature:  _____

**James B. Miller, Colonel, USMC
Director, Joint Advanced Warfighting School**

ABSTRACT

This study argues that the United States paradigm for the cybersecurity of critical infrastructure is flawed. For nearly two decades, repeated Presidential attempts, along with Congressional efforts, to revise cybersecurity policies result in new policies that contain old and unproven principles. Meanwhile, the cyber vulnerabilities within critical infrastructure information environments and the lethality of the global cyber threats to those national assets continue to grow. This research identifies and examines the foundational policy threads that resurface within consecutive Presidential cybersecurity policy initiatives over the previous twenty years. Collectively, these consistent themes constitute the United States' paradigm for cybersecurity. Although the United States' approach to cybersecurity cumulatively evolved during the past twenty years, its foundational principles remain unchanged, in error, and incapable of solving the nation's cybersecurity challenges. Specifically, two unproven beliefs, the Self-Regulation and Incremental Progress theories, remain consistent stalwarts throughout subsequent policies covering the cybersecurity of critical infrastructure. The United States requires revolutionary thinking to defend critical infrastructures against a twenty-first century cyber threat. Unfortunately, the traditional paradigm hinders innovative thinking about an evolving problem. The United States faulty cybersecurity paradigm rests upon unproven theories that left unchanged, trend the nation toward a national catastrophe.

This thesis examines the United States' evolution of cybersecurity policies through the lens of Thomas Kuhn's change theory. Thomas Kuhn's theory of change illuminates why two decades of national security policy continue to employ erroneous beliefs about securing the information environments that support national infrastructures. According to Kuhn, periodically a series of events creates a critical point in which the

long-held beliefs cease to resolve the complexities within an environment and create the conditions for a paradigm change. The United States is at just such an inflection point.

This thesis adds to the growing cybersecurity policy body of work by thoroughly examining the major cybersecurity policies beginning with the digital explosion of the late nineteen nineties. This thesis also identifies the flawed threads of policy that continually survive successive Presidential administrations. Ultimately, this study analyzes the cybersecurity environment and submits a fundamentally different paradigm for the cybersecurity of critical infrastructure. The new paradigm calls for a revision of commonly accepted cyberspace definitions, revitalizing the United States sensibilities for high risk/high pay-off technological innovations, an increased focus on creating inherently secure software, and the establishment of legislation targeted toward private owners of national critical infrastructures.

ACKNOWLEDGEMENT

First, and foremost, I would like to thank my entire family for their love, support and understanding. I am particularly grateful to my wife for her understanding and assistance in reviewing and editing this endeavor – Sweetheart, I love you!

I would also like acknowledge the students and instructors of JAWS, Seminar 2. Their collective insight and experience was instrumental to this year’s educational experience.

Specifically, I would like to thank COL Tom Rickard and Dr. Byron Greenwald. COL Rickard’s critiques of my countless cybersecurity ideas during countless hours of carpooling were very much appreciated. Finally, Dr. Greenwald’s theory and history lessons, as well as, his mentorship as a thesis advisor highly influenced my historical perspectives about the twenty-first century threat of cybersecurity.

TABLE OF CONTENTS

INTRODUCTION	1
CHAPTER 1: FOUNDATIONS.....	7
Evolution of ARPANet	7
What is Cyberspace?	15
The Cyber Threat Picture	24
Case Study: Stuxnet	32
CHAPTER 2: CYBER SPACE POLICY REVIEW	39
The Second Clinton Administration (1996-2000).....	40
The Bush Administration (2001-2008)	47
The Federal Information Security Management Act of 2002.....	48
The 2003 National Strategy to Secure Cyber Space.....	53
The First Obama Administration (2009-2012).....	58
The 2009 Cyber Space Policy Review	58
CHAPTER 3: RECOMMENDATIONS.....	62
Recommendation: Redefining Cyberspace	62
Recommendation: Game Changing Culture	65
Recommendation: Open Highway & Secured Exits	68
Recommendation: Limited Liability Legislation	71
CONCLUSION	75
BIBLIOGRAPHY.....	78
VITA	87

INTRODUCTION

The transition from a paradigm in crisis to a new one from which a new tradition of normal science can emerge is far from a cumulative process...Rather it is a reconstruction of the field from new fundamentals, a reconstruction that changes some of the field's most elementary theoretical generalizations, as well as, many of its paradigm methods and applications...When the transition is complete, the profession will have changed its view of the field, its methods, and its goals.¹ --Thomas S. Kuhn

This study argues that the United States paradigm for the cybersecurity of critical infrastructure is flawed. For nearly two decades, the United States has continued to employ cybersecurity principles that fail to protect critical infrastructure information environments from an evolving cyber threat.² Repeated Presidential attempts, along with Congressional efforts, to revise cybersecurity policies result in new policies that contain old and unproven principles. Meanwhile, the cyber vulnerabilities within critical infrastructure information environments and the lethality of the global cyber threats to those national assets continue to grow.

The technological explosion over the last twenty years, including the growth of the Internet, revolutionized the manner in which modern society processes, stores, and shares information. The United States' dependence upon interconnected information and computing technologies (ICT) is second only to its addiction to oil. Along with increased productivity and interconnectedness, Information Age societies face cyber related threats to the critical infrastructures that underpin their globalized economies. This research identifies and examines the foundational policy threads that resurface within consecutive Presidential cybersecurity policy initiatives over the previous twenty years. Collectively, these consistent themes constitute the United States' paradigm for cybersecurity.

¹ Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago: The University of Chicago Press, 1962), 84-85.

² Within this thesis the term cybersecurity strictly refers to the cyber defense of United States critical infrastructure.

Although the United States' approach to cybersecurity cumulatively evolved during the past twenty years, its foundational principles remain unchanged, in error, and incapable of solving the nation's cybersecurity challenges. Specifically, two unproven beliefs, the Self-Regulation and Incremental Progress theories, remain consistent stalwarts throughout subsequent policies covering the cybersecurity of critical infrastructure. The United States requires revolutionary thinking to defend critical infrastructures against a twenty-first century cyber threat. Unfortunately, the traditional paradigm hinders innovative thinking about an evolving problem. For example, the 112th Congress, armed with the aforementioned principles, voted down two excellent legislative bills (the Cybersecurity Act of 2012 and the SECURE IT Act of 2012) that would have improved the nation's cybersecurity of critical infrastructure posture. The United States faulty cybersecurity paradigm rests upon unproven theories that left unchanged, trend the nation toward a national catastrophe.

This thesis examines the United States' evolution of cybersecurity policies through the lens of Thomas Kuhn's change theory. Thomas Kuhn's theory of change, as detailed within *The Structure of Scientific Revolutions*, illuminates why two decades of national security policy continues to employ ineffective and erroneous beliefs about securing the information environments that support national infrastructures. *The Structure of Scientific Revolutions* presents 'normal science' and 'paradigm change' as disparate constructs for systematic advancement of knowledge and progress within a discipline.³ The United States cybersecurity paradigm is a product of the normal science

³ Although *The Structure of Scientific Revolutions* is widely credited for the term paradigm shift, Thomas Kuhn did not employ the term 'paradigm shift' in the book. Instead, Kuhn used the term 'paradigm change.' This thesis uses the terms paradigm change because change indicates a transformation to something fundamentally different from what it would be if left alone.

methodology. Communities of practice that employ the normal science methodology, dogmatically pursue solutions without challenging the widely acknowledged foundational beliefs.⁴ For example, consecutive Presidential Administrations created new cybersecurity initiatives without challenging the foundational principles that informed previous White House policy statements, U.S. legal code, Presidential Executive Orders, and Decision Directives. Periodically, a series of events creates a critical point in which the long-held beliefs cease to resolve the complexities within an environment and create the conditions for a paradigm change. The United States is at just such an inflection point.

The Structure of Scientific Revolutions warns that paradigm change is elusive and difficult because a community must first, conceptually recognize the methodology's inability to resolve complexities as true flaws, and second, endure a crisis that fractures the community into opposing thoughts.⁵ A paradigm change occurs only when a

⁴ Kuhn, *The Structure of Scientific Revolutions*, 10.

⁵ J. S. Bruner and Leo Postman, "On the Perception of Incongruity: A Paradigm," *Journal of Personality* 18 (1949): 206.

In a psychological experiment, subjects attempted to identify a series of playing cards presented in a short and controlled exposure pattern. Although most playing cards were traditional, some were anomalous. For example, the deck included a red six of spades or a black four of hearts. Each experimental session included the presentation of playing cards, one at a time, with gradually increased exposure times. After each card exposure, the researcher asked the subject what card he/she witnessed. Two successive correct identifications ended the session.

Most subjects correctly identified the traditional cards. However, the anomalous cards were almost always misidentified with conviction. The subjects often failed to observe anomalies. For example, participants confidently identified the black four of hearts as the four of either spades or hearts. Subjects routinely superimposed their personal experience paradigm when presented with an anomaly. Subjects appeared not to "see" or conceptually recognize deviations from their personal paradigm. When provided with extended exposure times, the subjects demonstrated apprehension when presented anomalies. However, hesitations did not produce the identification of the exact anomalies. Subjects would state, "That's the six of spades, but there is something wrong with it – the black has a red border."

While most subjects improved with multiple iterations, many never made the necessary adjustments. Some subjects demonstrated acute physical distress. One subject exclaimed, "I can't make the suit out, whatever it is. It didn't even look like a card that time. I don't know that color it is now or whether it's a spade or a heart. I'm not even sure now what a spade looks like."

community of professionals replaces a set of beliefs and principles, in whole or part, with a new theory.⁶ The crisis may present itself as an intellectual crisis or a physical catastrophe that forces the passion of the community and its stakeholders to demand change. Both Leon Panetta, former Secretary of Defense and Director of the CIA, and James A. Lewis, Director of the Center for Strategic and International Studies (CSIS) Technology and Public Policy Program, are among the nation's most vocal critics of the cybersecurity policy status quo. For example, during a 2011 interview, Secretary Panetta warned the nation about unseen threats that require a different approach to cybersecurity stating "... that there is the cyber capability to basically bring down our power grid...to paralyze our financial system in this country...to virtually paralyze our country."⁷ Likewise, Lewis' Congressional testimonies, published writings, and leadership at the CSIS place him at the forefront of innovative cybersecurity change agents. Lewis served as the Project Director for the highly influential 2008 report from the CSIS Commission on Cybersecurity for the 44th Presidency. The CSIS report presents over twenty recommendations that seek to challenge the validity of unproven paradigms, reframe the severity of cybersecurity threats, and advance a comprehensive cybersecurity policy agenda.⁸ While the CSIS report focuses on a broad range of cybersecurity topics to include offensive and international cybersecurity strategies, it doesn't analyze the specific challenges facing the cybersecurity of critical infrastructure.

The Structure of Scientific Revolutions indicates practitioners of a professional community behave in the same manner when anomalies appear among widely held paradigms.

⁶ Kuhn, *The Structure of Scientific Revolutions*, 92.

⁷ Scott Pelley, "Panetta: Cyberware could Paralyze U.S." CBS Interactive, Inc., http://www.cbsnews.com/8301-18563_162-57353420/panetta-cyber-warfare-could-paralyze-u.s/ (accessed October 28, 2012).

⁸ Center for Strategic International Security, *Securing Cyberspace for the 44th Presidency* (Washington DC: CSIS, 2008), 5-9.

This thesis adds to the growing cybersecurity policy body of work by thoroughly examining the major cybersecurity policies beginning with the digital explosion of the late nineteen nineties. This thesis also identifies the flawed threads of policy that continually survive successive Presidential administrations. These enduring principles create the paradigm that continues to place the nation, its infrastructure, and citizens at risk. Ultimately, this study analyzes the cybersecurity environment and submits a fundamentally different paradigm for the cybersecurity of critical infrastructure.

The scope of this thesis is limited solely to the cyber defense of critical infrastructure. Cybersecurity is a broad topic with multiple layers to include deterrence, attack, exploitation, and defense. Countless intertwined strands of friction exist within the various layers that collectively bind cybersecurity into a seemingly intractable knot. These interconnected strands include finance, privacy, international Internet governance, software development, and technology supply chain management to name only a few. This thesis focuses upon the policy framework to deter cyber attacks against critical infrastructure through *defense by denial*. Martin Libicki, in *Cyberdeterrence and Cyberwar*, adeptly articulates the intricate relationship between defense and deterrence:

If deterrence is anything that dissuades an attack, it is usually said to have two components: deterrence by denial (the ability to frustrate the attacks) and deterrence by punishment (the threat of retaliation).⁹

William Kaufman, special assistant to each Secretary of Defense from 1961 to 1981, authored the counterforce nuclear deterrence theory. The theory, described below, highly influences this author's fundamental understanding of defense as a central pillar to any deterrence concept:

⁹ Martin Libicki, *Cyberdeterrence and Cyberwar* (Arlington: RAND Corporation, 2009), 7.

Deterrence consists of essentially two basic components: first, the *expressed intention* to defend a certain interest; secondly, the *demonstrated capability* actually to achieve the defense of the interest in question or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort to him.¹⁰

Defense by punishment, counterattack, or preemptive attack are critical and necessary ingredients for cyber deterrence. However, offensive and punitive cyber attack strategies are beyond the scope of this research. The use of the term cybersecurity within this thesis always refers to cyber defense. The author understands and accepts cyber defense as merely a single component to an effective cybersecurity policy.

Chapter 1, Foundations, provides the building blocks of cyber understanding through an examination of the Advanced Research Project Agency's impact upon national interests and the creation of the Internet. This chapter also includes rationale for the author's revised cyberspace definition, along with a Stuxnet Case Study that highlights the growing cyber threat to critical infrastructures. Chapter 2, Cyberspace Policy Review, conducts an examination of the United States cybersecurity policy and identifies the consistent themes throughout the past three Presidential administrations that continue to slow progress. Finally, Chapter Three, Recommendations, submits principles for a new United States cybersecurity paradigm.

¹⁰ Adam Bernstein, "Obituaries: Defense Expert William Kaufmann," *Washington Post*, December 17, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/16/AR2008121602724.html> (accessed January 15, 2013). (*emphasis added*)

In 1954, Secretary of State John Foster Dulles advanced the "massive retaliation" nuclear strategy. In the same year, William Kaufmann published the essay, "The Requirements of Deterrence," that harshly criticized Dulles' strategy. Mr. Kaufmann then controversial essay stated, "We must face the fact that, if we are challenged to fulfill the threat of massive retaliation, we will be likely to suffer costs as great as those we inflict." In 1960, Mr. Kaufmann proposed the "counterforce" strategy, which unlike massive retaliation, fired its first volley of nuclear weapons at Soviet bomber bases and submarine pens in an effort to avoid Soviet cities. The limited response strategy sought to bring a nuclear war to a resolution shy of mutual annihilation. Mr. Kaufmann persuaded several Secretaries of Defense that counterforce provides a wider variety of Presidential options in contrast to the massive retaliation strategy.

CHAPTER 1: FOUNDATIONS

Evolution of ARPANet

The history of the Advanced Research Project Agency (ARPA) and the ARPA Network (ARPANet) provide context into twenty-first century cybersecurity challenges and markers toward potential solutions. On October 4, 1957, the Soviet Union's launching of the world's first intercontinental ballistic missile, with the first artificial satellite onboard, Sputnik, thrust the United States into intellectual crisis.¹ Sputnik awakened the United States from its assumption of hegemonic technological prowess and spurred increased funding for scientific research, education, and development.² Then Senate Majority Leader Lyndon B. Johnson and future President remarked, "Now, somehow, in some new way, the sky seemed almost alien. I also remember the profound shock of realizing that it might be possible for another nation to achieve technological superiority over this great country of ours."³ The launch of Sputnik signaled serious problems within the United States' management of science and technology research.⁴ The United States required a fundamentally new approach to science and technology research. The United States' response to the need for innovation was the creation of the Advanced Research Project Agency.

¹ Richard Van Atta, *50 Years of Innovation and Discovery* (Washington DC: DARPA), www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2553 (accessed January 28, 2012).

² Gary Anthes, "Happy Birthday Sputnik!" *Computerworld* 41, no. 44 (October 2007): 44-46, <http://search.proquest.com.ezproxy6.ndu.edu/docview/216118814?accountid=12686> (accessed March 3, 2013).

³ Van Atta, *50 Years of Innovation and Discovery*.

⁴ Anthes, "Happy Birthday Sputnik!" 44-48, 50.

In 1958, President Dwight Eisenhower created ARPA, within the Department of Defense, in response to the launch of the Russian satellite Sputnik.⁵ ARPA's purpose was to reestablish and maintain the United States' technological preeminence over potential enemies and prevent technological surprise.⁶ The agency, since renamed the Defense Advanced Research Projects Agency (DARPA), later expanded its mission to include creating technological surprise for potential enemies.⁷ From the beginning, national leaders recognized the need for an agency with a unique culture capable of reaching beyond the cumulative and incremental methodologies associated with normal science development.⁸ The Defense Advanced Research Projects Agency's culture, outlined below in its three attribute concept, rewards critical and creative thinking:

- **Independence.** DARPA research and development efforts focus *beyond* next generation technologies. Neither DARPA Program Managers nor selected projects derive from explicit military service component requirements.
- **Risk Taking.** The DARPA Director selects research projects and Program Managers capable of high risk/high payoff concepts. DARPA is a high performance learning organization that remains unafraid of failure. DARPA's organizational structure is lean, decentralized, and aggressive. In fact, DARPA owns zero laboratories. The Director's office pushes decision making, initiative, and responsibility down to Program Managers within the nation's leading research laboratories. Program and Project Managers both conceive and manage all of DARPA's initiatives.
- **Idea Driven & Outcome Oriented.** Promising ideas are the currency of DARPA selected projects. Program Managers identify projects and convince the Board of Directors of their high potential. DARPA selects projects void of well-proven notions, while never pursuing projects for the pure pursuit of

⁵ Anthes, "Happy Birthday Sputnik!" 44-48, 50.

⁶ Ibid.

⁷ Defense Advanced Research Projects Agency, "About DARPA," DARPA, <http://www.darpa.mil/About.aspx> (accessed September 21, 2012).

In 1972, Congress renamed ARPA (Advanced Research Projects Agency) DARPA (for Defense), then back to ARPA in 1993, and again renamed to DARPA in 1996.

⁸ Van Atta, 50 Years of Innovation and Discovery.

science. Project goals vary from demonstrating an idea's technical feasibility to providing proof of concept for an operational capability.⁹

Throughout its history, DARPA catalyzed and assured the United States' position as the world's technological hegemon. The Advanced Research Project Agency's history and culture uniquely qualifies the agency to once again lead the nation against the growing cybersecurity problem set.

The Advanced Research Projects Agency is the catalyst for much of cyberspace and it must now lead the nation in securing cyberspace. ARPA computer scientists pioneered the Advanced Research Projects Agency Network (ARPANet), the precursor to the Internet, within an information environment void of nefarious actors.¹⁰ The ARPANet research community included a select group of well-known research participants, mainframes, and terminals.¹¹ ARPANet pioneers developed a blind spot against the need to develop inherently secure technologies due to the uncontested information environment.¹² In fact, ARPANet engineers faced complex challenges that focused their efforts on the interoperability and productivity of communication technology and led them to miss the need for holistic security.¹³ The developed technological solutions to ARPANet's early challenges serve as the underpinnings of the modern Internet.

⁹ Ibid. (emphasis added)

¹⁰ Jennifer DiSabatino, "The Wild Wild West," *Computerworld* 35, no. 46 (November 2001), <http://search.proquest.com.ezproxy6.ndu.edu/docview/216089759?accountid=12686> (accessed March 9, 2013).

¹¹ Ibid.

¹² President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure* (Washington DC: Government Printing Office, October 1997), 16.

¹³ Ibid.

Therefore, without a fundamentally new approach to the science of cybersecurity, the Internet and cyberspace will remain less secure than the laws of science demand.¹⁴

In 1962, ARPA leadership created the Information Processing Techniques Office (IPTO), since renamed Innovation Information Office, to fund and manage computer science projects.¹⁵ Since its inception, the IPTO's computer research project management record is remarkable. The IPTO is the historical driving force behind many of the world's ground breaking computing science research developments, including the first distributed information network, the first successful email message, and the first graphical user interface (GUI) computer program.¹⁶ The first IPTO Director, Joseph Carl Robnett Licklider, authored a series of memorandums (later termed the "Galactic Network" memos), which are widely considered the first recorded plan for a digital communication network.¹⁷ One particular memorandum warned that the project may "never become anything more than a high-tech Tower of Babel, in which widely scattered enclaves produced incompatible machines, incompatible languages, and incompatible software."¹⁸ By 1966, Robert Taylor, the third IPTO director, realized Licklider's fears. Processes and technologies among IPTO's three participating research

¹⁴ The MITRE Corporation, *Science of Cybersecurity* (Rosslyn, VA: The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2010), www.fas.org/irp/agency/dod/jason/cyber.pdf (accessed March 19, 2013).

¹⁵ Janet Ellen Abatte, "From ARPANet to Internet: A History of APRA-Sponsored Computer Networks, 1966-1988" (PhD diss., University of Pennsylvania, 1994), <http://search.proquest.com.ezproxy6.ndu.edu/docview/304104775?accountid=12686> (accessed March 28, 2013).

¹⁶ Gary Anthes, "Timeline: Sputnik and Three Decades of DARPA Hegemony," Computerworld (Online), http://www.computerworld.com/s/article/9037638/Timeline_Sputnik_and_Three_Decades_of_DARPA_Hegemony (accessed February 7, 2013).

¹⁷ Mitch Waltrip, *DARPA and the Internet Revolution* (Washington DC: DARPA), www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554 (accessed October 15, 2012), 79.

¹⁸ Ibid.

universities were duplicative, incompatible, and stove-piped.¹⁹ Additionally, the level of information sharing between universities was nearly non-existent. Collectively, the lack of interoperable software languages and non-scalable technologies served as the problem statement and catalyst for solutions that drove ARPA toward the need for a communications network. It was clear that proprietary and closed-source information and communication technologies (ICT) promoted incompatibility and inefficiency. In fact, Taylor maintained three disparate desktop terminals within his office in order to communicate with three incompatible ARPA-funded research university computing systems.²⁰ Taylor later remarked, “Anyone in that context would have quickly thought, ‘Hey, wait a minute, why can’t I get to any of these places from one terminal?’”²¹

In 1967, the IPTO director hired Larry Roberts to lead the Advanced Research Projects Agency Network (ARPANet) project.²² The project’s goal was to employ communications technologies that allowed research institutions to share computing resources.²³ Mr. Roberts’ decisions to employ packet switching and decentralized routing structures enabled a common communications structure and forever shaped the Internet, cyberspace and cybersecurity.²⁴

Robert’s first action was to abandon circuit switching technologies, the prevalent communication protocol, in favor of newly validated packet switching technologies. Circuit switching technologies resemble a multilane highway in which the painted lines

¹⁹ Waltrip, DARPA and the Internet Revolution, 80.

²⁰ Ibid.

²¹ Ibid.

²² Ibid.

²³ Ibid.

²⁴ Ibid.

are solid.²⁵ In a circuit switched network, each call (data, voice, or video) receives and maintains exclusive and full use of its own lane. For example, during a circuit switched telephone call, the caller pays for the entire “air time” to include breaks and lulls in the conversation. Since the communication link is dedicated and unavailable to other users, the caller incurs the complete cost. The primary advantages of circuit switching are (1) non-repudiation of transmissions and (2) the clarity and stability of each connection. Employing dedicated circuits for the sporadic nature of digital data transfer is inefficient because of its inability to constantly and consistently saturate any one circuit.²⁶

Packet switching technologies, including Transmission Control Protocol and Internet Protocol (TCP/IP), resemble a multilane highway in which the painted lines are dashed lines.²⁷ Packet switching separates transmissions into smaller pieces (packets) of data and disperses them among separate lanes.²⁸ Instead of exclusive ownership of an

²⁵ Seth Schiesel, “AT&T’s Embrace of New Technology Signals Next Era.” *New York Times*, March 8, 1999, <http://search.proquest.com.ezproxy6.ndu.edu/docview/431147861?accountid=12686> (accessed August 10, 2012).

²⁶ Ibid.

²⁷ Ibid.

²⁸ Curt White, *Data Communications and Computer Networks: A Business User's Approach*, 4th ed. (Boston: Thomson Course Technology, 2007), 338-341.

Internet services (email, web pages, links, remote login) are enabled by a series of packet switching technologies. The TCP/IP protocol suite and the Open Source Interconnection (OSI) model are frameworks used to describe and categorize network technologies. Countless network technologies comprise the frameworks to include Hypertext Transfer Protocol (HTTP), Dynamic Host Configuration Protocol (DHCP), and User Datagram Protocol (UDP) among others. However, the two dominant protocols of network technology and the Internet are Transmission Control Protocol (TCP) and Internet Protocol. These protocols are the foundation of communication networks to include the Internet.

Internet Protocol (IP) provides a connectionless (think opposite of circuit switching) data transfer service over a disparate networks by passing and routing data packets. The IP protocol encapsulates data packets with the information necessary to transport data packet at the origin and unencapsulate the data packet for reassembly with other packets at the destination. The necessary information includes origin and destination address information, data packet size, and the date/time the packet was created. Routers analyze IP information to determine the desired packet traffic path, further fragment the packet depending on the size of the forwarding network, and if necessary delete the packet.

Transmission Control Protocol (TCP) performs functions to increase the stability and reliability of network transmission through network connection error checking. A TCP header is encapsulated into data

entire lane, packets from the same transmission enter multiple lanes with other separated packets and reassemble at or near the destination. The primary advantages of packet switching include the potential (1) to maximize a lane's capacity (bandwidth) and (2) to transmit mammoth quantities of packets to geographically dispersed destinations.²⁹ The disadvantage of packet switching is the difficulty of attributing responsibility of a message to its originator. However, the ARPANet research community was small, trusted, and well-known within the community of researchers.³⁰ The ARPANet project community only consisted of three exclusive research universities of known and trusted engineers.³¹ Therefore, Roberts's project challenges were void of information security concerns, but centered on productivity and interoperability of dispersed and disparate information systems.

Next, Roberts decentralized ARPANet's routing of data packets. Although decentralized routing adds a layer of user anonymity, it increases the speed and reliability of networked computing. ARPANet's routing design relied upon the concept of shared responsibility among network computers (routers).³² Although a centralized architecture is easier to design and maintain, centralization also breeds single points of catastrophic failure.³³ ARPANet implemented peer routers, then called Interface Message Processors, to sort and route packets from origins to destinations. ARPANet employed matrix

packets that perform several stability and reliability functions. The encapsulated header functions include the creation of a connection between a sender and receiver, connection acknowledgement and error checking, release of the connection after all data is sent, and prioritization of data packets such as error checking packets.

²⁹ Schiesel, "AT&T's Embrace of New Technology Signals Next Era."

³⁰ DiSabatino, "The Wild Wild West."

³¹ Waltrip, DARPA and the Internet Revolution.

³² Ibid.

³³ Ibid.

architecture with adaptive packet switching technologies capable of determining the most efficient transport path for each packet. The unintended consequence of packet switching technologies is the presence of near anonymous Internet activity among its users. In fact, accurately identifying users within a packet switched environment, absent the use of digital signatures, remains nearly impossible.³⁴

Pioneering network computer engineers designed ARPANet as a collaborative communications platform containing efficient and interoperable technologies. Interoperability and efficiency were the prime goals, not security, during the development of Internet software protocols.³⁵ Communications protocols, along with a decentralized architecture, contribute to the anonymous nature of Internet travel. Internet designers valued efficient data flow over information confidentiality, data integrity and identity authentication.³⁶ Considering the uncontested security environment and challenges to efficiency and interoperability, it is unreasonable to believe early network pioneers could have foreseen the information security challenges of the twenty-first century.³⁷ The anonymous character of Internet communications protocols remains a challenge to reducing cybersecurity risks to manageable levels.

³⁴ Harry Newton, *Newton's Telecom Dictionary*, ed. Steve Schoen, 25th ed. (New York: Flatiron Publishing, 2009), 370.

A digital signature is the network equivalent of hand written signature that prevents the creator from denying authorship of the source document and assures the recipient of its origin. A digital signature is an electronic signature that is extremely difficult to forge. Receiving a message with a digital signature provides an extremely high level of confidence that the document has not been altered since it was signed.

³⁵ Kamlesh Bajaj, *The Cybersecurity Agenda: Mobilizing for International Action* (New York: East West Institute, 2010), <http://www.ewi.info/cybersecurity-agenda> (accessed November 13, 2012), 6.

³⁶ *Ibid.*

³⁷ U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington DC: Government Printing Office, July 2011), 2.

ARPANet is the precursor the modern interconnected communications network now termed the Internet. However, cyberspace, and therefore cybersecurity, is much broader than the Internet. Policy often mistakenly equates the Internet with cyberspace. While effective Internet security is necessary to reduce cyber vulnerabilities, separating critical infrastructure information systems from Internet connection does not guarantee freedom from cyber threats. The section below examines the definition of cyberspace and presents the author's revised definition. The section seeks to illuminate incomplete cyberspace definitions that misinform cybersecurity policy. A functional definition provides both cybersecurity strategist and national policy makers a contextual foundation for the development of appropriate policy.

What is Cyberspace?

The United States must communicate and operate from an accurate definition of cyberspace in order to develop effective cybersecurity of critical infrastructure policy. Author William Gibson first coined the term cyberspace in the 1982 science fiction novel, *Burning Chrome*, by combining the words cybernetics and space.³⁸ In 1984, Gibson popularized the term in his following novel *Neuromancer*, where he described cyberspace as, “A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data.”³⁹ The original descriptions of cyberspace do little to advance the policy strategist requirement to demystify the domain.

³⁸ Kamal Jabbour, *50 Cyber Questions Every Airman Can Answer* (Rome, NY: Air Force Research Laboratory, 2008), 3.

³⁹ *Ibid.*

However, this section seeks to provide a clear cyberspace definition that informs policy creation.

This section presents a revised cyberspace definition that demystifies the nature of the global domain. In *War and Anti-War*, co-authors Alvin and Heidi Toffler wrote, “The way we make war reflects the way we make wealth, and the way we make anti-war (diplomacy) must reflect the way we make war.”⁴⁰ All societies, whether agrarian, industrial, or knowledge-based, generate instruments of power reflective of their wealth source.⁴¹ The United States projects its diplomatic, information, military and economic instruments power from the superior ability to create, collect, and synthesize massive knowledge stores. This section defines cyberspace as an engineered domain instead of a naturally occurring scientific phenomenon such as land, sea, or air. Many policy makers mistakenly equate cyberspace with the Internet and categorize it as a naturally occurring global common. Poor definitions drive policy makers to develop misaligned strategies incapable of achieving policy objectives. This study presents two current cyberspace definitions and suggests a revised definition, along with rationale for the new characterization.

In *Third Wave*, the Tofflers accurately predicted the emergence of twenty-first century Information Age societies.⁴² Information Age societies leverage data and computing technologies to create actionable knowledge capable of solving complex and

⁴⁰ Alvin Toffler and Heidi Toffler, *War and Anti-War*. (New York, NY: Little, Brown & Company, 1993), 2.

⁴¹ Ibid.

⁴² Nathan Gardels, "He Has Seen the Future," *Financial Times*, August 19, 2006, <http://www.ft.com/cms/s/0/af33b982-2dbd-11db-93ad-0000779e2340.html#axzz2Lm4HX9cn> (accessed October 5, 2012).

evolving problems.⁴³ Cyberspace is the collective convergence of engineered technologies that fuel post-Industrial Age societies. Information and computing technologies, such as TCP/IP and underwater fiber-optic cabling, underpin Information Age societies and knowledge-based economies. By 2015, information and computing technologies will facilitate the connection of over one trillion devices to the Internet.⁴⁴ Additionally, knowledge-based economies are likely exiting the Information Age and embarking upon an unnamed post-Information age marked by the convergence of biology and computer engineering.⁴⁵ This thesis accepts cyberspace as a global domain, but stops short of acknowledging cyberspace as global common due its engineered nature. The engineered nature of cyberspace provides credence toward the pursuit of game changing technological solutions to cybersecurity challenges.

The Department of Defense (DoD) leads all United States government agencies in its understanding and attention to cyberspace. The 2010 Quadrennial Defense Review Report (QDR) accurately captured the essence of cyberspace when stating, “Although it is a *man-made domain*, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space....The Administration will

⁴³ Ibid.

⁴⁴ Ayesha Khanna and Parag Khanna, "Technology Will Take on a Life of its Own," *Foreign Policy*, no. 188 (September/October, 2011): 2.

In 2011, “Watson,” the famed IBM artificial intelligence (AI) computer, outperformed both Grand Jeopardy Champions on national television. “Watson” exhibited the two highest markers of human intelligence: contextual understanding and language comprehension. Converging technologies such as biotechnology and artificial intelligence will change entire civilizations to include their security environment. The security environment will undergo chaos while advanced societies attempt to transition into the unnamed post-Information Age and leave lessor developed societies behind.

⁴⁵ Quentin Duroy, "The Place of Biotechnology in Modern Civilization: A Veblenian Analysis of Public Misgiving Toward Embryology in the United States," *Journal of Economic Issues* 45, no. 3 (September 2011): 559.

Early indicators of the an impending post-Information age, characterized by the convergence of humans and technology are emerging. For example, only moral objections currently stand between biotechnology and successful human cloning.

continue to explore the implications of cyberspace's unique attributes for policies regarding operations within it."⁴⁶ However, the Department of Defense's cyberspace definition (listed below), while useful, does not explicitly identify cyberspace's purpose and places an inordinate level of emphasis upon communications networks.

The human engineered global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.⁴⁷

The purpose of cyberspace is to perform valuable information functions. An explicit purpose within the definition provides a context that facilitates the ability of national security policy makers to think critically about the "why" of security challenges. Unfortunately, the DoD definition mistakenly elevates interdependent networks, such as the Internet, as the linchpin of cyberspace. In reality, software code is the engine that drives every information and computing *system* within cyberspace, including the Internet.

The Center for Technology and National Security Policy (CTNSP), an arm of the National Defense University, presents an effective and more granular definition of cyberspace.

A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies.⁴⁸

⁴⁶ U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington DC: Government Printing Office, February 2010), 37. (*emphasis added*)

⁴⁷ U.S. Department of Defense, *Department of Defense Dictionary of Military Terms and Associated Terms* (Washington DC: Government Printing Office, November 2012), 77.

⁴⁸ Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 1st ed. (Dulles, VA: Potomac Books, 2009), 28.

The CTNSP definition is extremely useful because it highlights the purpose of cyberspace activity. The desire and ability of organizations to “create, store, modify, exchange and exploit information” provides focus to cybersecurity practitioners and national security policy makers. Several information and computing technology *systems*, beyond Internet technology, work collaboratively to “to create, store, modify, exchange, and exploit information.” Therefore, effective cybersecurity of critical infrastructure policy is not equivalent to effective Internet security policy. Instead, cybersecurity policy, and therefore the supporting definitions, should focus squarely upon information systems and the software codes that enable valued information and their critical industrial processes.

A cybersecurity policy that overemphasizes Internet security is misguided. In fact, the United States benefits more from an open and interoperable Internet than any nation in the world. Economic globalization and the Arab Spring are direct descendants of an open and interoperable Internet. The alternative to an open and interoperable Internet is a fragmented information environment, in which nation states restrict access to advanced technologies, streaming media, and sophisticated software under the guise of national security interests.⁴⁹ For example, in 2011, former Egyptian President Hosni Mubarak’s regime closed the Egyptian population’s access to the global Internet following massive demonstrations.⁵⁰ Journalists and activists lost the ability to

⁴⁹ U.S. President, *International Strategy for Cyberspace* (Washington DC: Government Printing Office, May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed August 15, 2012), 8.

⁵⁰ Karson K. Thompson, "Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate," *Texas Law Review* 90, no. 2 (2011): 465, <http://search.proquest.com.ezproxy6.ndu.edu/docview/916011879?accountid=12686> (accessed October 4, 2012).

communicate globally through social networking sites such as Twitter, Facebook and YouTube.⁵¹ The world's information superhighway, the Internet, contains exit ramps that lead to countless global assets to include critical infrastructures within the United States. This study supports the hardening of critical off ramps that lead to critical information systems, while allowing the benefits and risks of an open and anonymous global information superhighway that fuels democratization and globalization. Therefore, an effective cyberspace definition must focus on information systems, of which the Internet is a component, that are underpinned by lines of software code. While largely accurate, neither the DoD nor the CTNSP definitions conveys the essential role of software code to cyberspace.⁵² Software code, not the Internet, is the valued asset that is targeted and defended by the hacker and system owner respectively. Software code is the genesis of every benefit, vulnerability, and threat within the information environment termed cyberspace. Below is the author's revised cyberspace definition:

The global domain within the information and communications environment consisting of communication links, hardware, and software necessary to create, modify, store, and exchange information and control computing systems; Software code is acknowledged as the central element among the three critical components that direct and control information and computing systems.

The revised definition contains three noteworthy distinctions and serves as a foundation for this thesis. First, the definition identifies communication links, hardware, and software as essential components of cyberspace. Poor cyberspace definitions and metaphors often mistakenly equate cybersecurity with Internet security. The Internet is a global communication network comprised of many small, medium, and large

⁵¹ Ibid.

⁵² Khanna and Khanna, "Technology Will Take on a Life of its Own," 2.

interconnected networks. Simply stated, the Internet is a networked transport path (superhighway) for varying sized information packets (cars, motorcycles, cargo vehicles) to reach desired hardware (homes, office buildings) that contain valued information and/or critical information systems (Assets: money, families, inventory) controlled by software (people). Although responsible cybersecurity policy must address Internet security, cyberspace is much broader than the Internet. Cybersecurity is not wholly reliant upon effective Internet security. The Stuxnet Case Study presents a scenario in which an organized hacker attacked critical infrastructure systems unconnected to the global Internet. The lack of Internet connectivity to a critical information source or process does not insulate an information system from a determined adversary. Therefore, equating cyberspace to the Internet mistakenly implies the sufficiency of Internet security as effective cybersecurity.

Second, the revised definition explicitly states the purpose of cyberspace as the ability “to create, modify, store, and exchange information and/or control computing systems.” The various information and computing functionalities serve as the purpose for human entry into cyberspace. Understanding functionalities, and therefore cyberspace purposes, provides the needed insight and context for understanding cyber actors, tactics, and desired effects. Information and computing technologies leveled the playing field for underfunded and undersized organizations. Underfunded groups produce effects formerly reserved for nation-states and large corporations. For example, compression technologies provide individuals and small groups with the ability to manipulate data inexpensively to achieve an effect.⁵³

⁵³ Newton, *Newton's Telecom Dictionary*, 304.

Compression technologies remove indiscernible information from a picture, video or audio file. Without compression technology, video production, streaming media and data sharing becomes too costly for all except well-funded organizations. For example, the February 2007 edition of Technical Mujahid contained an article that encouraged extremists to download a copy of an encryption program "Secrets of the Mujahideen" from the Internet.⁵⁴ The program compressed and hid messages within pixels to defeat steganalysis attempts.⁵⁵ As more societies enter the Information Age, the expansion of individually produced and manipulated content will grow exponentially. In fact, according to the Internet World Statistics, the percentage of Internet users among the world population grew from 28.7% (1.9 Billion) in June 2010 to 32.7% (2.3 Billion) in December 2011.⁵⁶ The capability to create, modify, store, and exchange information for the purpose of creating a strategic effect is no longer the sole province of nation-states and large corporations.

Audio waves are the most commonly known type of compressed information. Data intense audio waves from the recording studio are squeezed into a CD. In order to make a MP3 file for an iPod, the file is compressed a second time. The compression process removes audio waves that are indiscernible to the human ear. Lossless techniques compress without removing detail; lossy compression techniques compress data by removing detail. During the compression of video files, bits of indiscernible video are eliminated by removing detail, color, or identical successive frames. Compression reduces the bandwidth, memory and processing power required to transmit, store and encapsulate a file respectively. These efficiencies reduce the costs to produce and share large amounts of content.

⁵⁴ Marthie Grobler and Namosha Veerasamy, "Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure," (lecture presented at the 6th International Conference on Information Warfare and Security, George Washington University, Washington DC, March 17-18, 2011), <http://researchspace.csir.co.za/dspace/handle/10204/5781>. (accessed October 31, 2012), 6.

⁵⁵ Newton, Newton's Telecom Dictionary, 1058.

Steganography is a method for encoding hidden messages into the least significant bit of other files, such as graphic, audio and HTML files, which have large amounts of unused space. Once the data is encoded, it can be decoded with the correct password. Steganalysis is the art and science of detecting messages hidden using steganography.

⁵⁶ Internet World Stat, "Internet World Stat: Usage and Population Statistics as of December 31, 2011," Miniwatts Marketing Group, <http://www.internetworldstats.com/stats.htm> (accessed November 1, 2012).

Third, the revised definition highlights software code as the “central element among the three critical components which directs and controls information and computing systems.” Software code is the valued prize of the cyber hacker. The valued information or computing process is not the hardware or the communication link. The most successful cyber attacks are dedicated to finding, exploiting, disrupting or destroying unknown vulnerabilities, called zero day vulnerabilities, within software.⁵⁷ Software represents both the brains of computing productivity and the primary source of vulnerability. While most cybersecurity literature focuses upon Internet security, there is no defense for zero day software vulnerability.⁵⁸ The software development life cycle favor a first to market strategy that produces “good enough” security features, which require countless subsequent software patches. The software’s customer base discovers many software vulnerabilities that require patches and upgrades. The customer base supplements the software developer’s research and development costs.⁵⁹ Hackers also research and target zero day vulnerabilities within commercial off the shelf (COTS) software such as Internet Explorer, Blackberry Enterprise Server, and mostly widely used operating system in the world, Microsoft Windows. Leading software security firms, McAfee, Symantec, Norton and Kaspersky, reverse engineer malicious software, identify the virus’ signature, and create an algorithmic hash for identified software vulnerabilities.

⁵⁷ Jeffrey Carr, *Inside Cyber Warfare*, ed. Mike Loukides, 1st ed. (Sebastopol, CA: O’Reilly Media Incorporated, 2009), 152.

Zero Day Attack: An attack against a software vulnerability that is unknown to the software creator. In the world of computer security, zero-day vulnerabilities signal that the attacker is a professional. Unknown software vulnerabilities are exploited for a variety of purposes. Knowledge of and software directed against zero day vulnerabilities sell on the black market for as much as \$100K.

⁵⁸ *Ibid.*, 158.

⁵⁹ David Rice, *Geekonomics: The Real Cost of Insecure Software*, (Boston, MA: Pearson Education, 2008), Kindle E-Book, Chapter 2. (*emphasis added*)

Signature-based anti-virus software is only effective against known malicious software code. Therefore, signature-based anti-virus software is only effective *after* the initial zero-day exploit.⁶⁰ The software development industry creates inherently unsecure software code, which makes traditional cybersecurity strategies reactionary at best.

The manner in which national policy defines cyberspace drives the development of solutions that address cybersecurity challenges. Cyberspace definitions and metaphors must acknowledge the role that software plays within the broader context of information and computing technology systems. Equating the Internet with cyberspace undermines the nation's understanding of the information environment. An open and interoperable information superhighway is necessary to fuel the growth of emerging economic and political interests. However, malicious actors with sophisticated tactics seek to penetrate valued assets to include United States critical infrastructures. The section below details the cyber threat facing the United States' critical infrastructure.

The Cyber Threat Picture

Verizon Business publishes an annual Data Breach Investigations Report (DBIR) that aggregates cyberspace intrusion data collected from several international law enforcement agencies. Participating organizations include the United States Secret Service, the Australian Federal Police, the Dutch National High Tech Crime Unit, the Irish Reporting and Information Security Service, and the United Kingdom Police Central

⁶⁰ Shon Harris, *CISSP: All in One Exam Guide*, ed. Timothy Green, Joe Hoofnagle, and Clement Dupuis, 4th ed. (New York: McGraw-Hill, 2008), 1001.

e-Crime Unit.⁶¹ The 2012 report chronicled 855 cyber intrusions that included over 170 million compromised information records.⁶² The 2012 study represents the second highest level of data loss since the initial 2004 report.⁶³ The DBIR employs an excellent threat model, titled the Verizon Enterprise Risk and Incident Sharing (VERIS) framework that depicts cyber actors, targets, tactics, and effects within a multi-dimensional spreadsheet. The VERIS framework assists in reducing the inherent complexity of cyber threats. The VERIS framework is extremely useful and can be used to record intrusion effects within servers, networks, user devices, offline data, and people. The first dimension consists of actors and hackers that carry out malicious cyber behavior. The second dimension includes the tactics, techniques and procedures (TTPs) employed by hackers. Finally, the third dimension includes the range of a hacker's desired objectives and effects.

The delineation among the various cyber hackers is largely drawn along the lines of intent and motivation. Additionally, cyber hackers operate behind the veil of anonymity that creates an asymmetric cybersecurity environment. Within cyberspace, the defenders risk and cost severely outweigh those of the attacker. For example, a low cost USB device containing one single malicious code is capable of disrupting an enterprise data center. However, the data center owner assumes great risk and cost to defend and harden the information assets against a wide variety of cyber tactics, techniques and procedures. While accurate attribution of cyber incidents to responsible

⁶¹ Verizon Business, *2012 Data Breach Investigation Report* (Ashburn: Verizon Business, 2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (accessed September 21, 2012).

⁶² Ibid.

⁶³ Ibid.

parties is essential to an effective cybersecurity policy, cyber intrusion investigations should begin with an understanding of the actor's intent and motivations. Table 1, Hacker Motivations, describes the most common malicious cyber actors.

<u>Actors/Hackers</u> ⁶⁴	<u>Motivations and Primary Tactics</u>
Nation States (Foreign Intelligence and/or Militaries)	Nations conduct information gathering, espionage, and attacks against critical infrastructures. According to the GAO, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. ⁶⁵ A growing array of state adversaries increasingly target enterprise data centers, communication infrastructures, computer systems, firmware, and embedded processors within critical industries for exploitation, disruption or destruction. ⁶⁶
Organized Criminals	Criminal groups penetrate information systems to conduct theft, fraud, and extortion. Corporate spies leverage similar tactics and pose a threat to the United States through their ability to acquire data gained from extensive research and development. ⁶⁷
Hacktivists	Hacktivists are motivated by political objectives and target publically accessible Web pages or email servers in order to advance their message or subdue an adversary's information message. Hacktivists are likely to overload individual email accounts and enterprise email servers and/or flood email accounts with political messages. ⁶⁸
Terrorists	Terrorists are currently less developed in computer network capabilities than nation states and are likely to target critical infrastructure to cause mass casualties, weaken the U.S. economy, and damage public confidence. ⁶⁹

Table 1: Hacker Motivations

The quantity and sophistication of cyber attack tactics continues to grow at an alarming rate. In fact, the exact quantity of cyber attack variants is unknown due to an

⁶⁴ Robert O'Harrow, "Hacking Tool Kits, Available Free Online, Fuel Growing Cyberspace Arms Race." *Washington Post*, November 13, 2013, http://www.washingtonpost.com/investigations/hacking-tool-kits-available-free-online-fuel-growing-cyberspace-arms-race/2012/11/12/1add77a4-21e6-11e2-ac85-e669876c6a24_story.html?wpisrc=emailtoafriend (accessed November 15, 2013).

Within this thesis, the terms actor and hacker are used interchangeably. Hackers are motivated by various factors to include financial, political, prestige, or espionage. Hacking once required high levels of skill. Now, hackers can purchase or download sophisticated attack scripts from the Internet and launch them against victim sites.

⁶⁵ Government Accounting Office, *Cybersecurity: Threats Impacting the Nation*, by Gregory Wilshusen (Washington DC: Government Printing Office, 2012), 3-13.

⁶⁶ Ibid.

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ Government Accounting Office, *Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities*, by David D'Agostino and Gregory Wilshusen (Washington DC: Government Printing Office, 2011), 13.

explosion of pre-packaged illicit cyber attack kits for sale on the global hacker black market.⁷⁰ H.D. Moore, Chief Security Officer for Rapid7, a leading manufacturer of vulnerability management and penetration testing software, states that pre-packaged malicious software routinely sells for up to \$100,000.⁷¹ The tactics available to software programmers and malicious actors are infinite. Table 2, Hacker Tactics, Techniques and Procedures, includes the most common tactics employed in cyberspace.

⁷⁰ O'Harrow, "Hacking Tool Kits, Available Free Online, Fuel Growing Cyberspace Arms Race".

⁷¹ Joseph Gross Michael, "A Declaration of Cyberwar," *Vanity Fair*, April 2011, <http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/919475999?accountid=12686> (accessed November 19, 2012).

<u>Tactics</u>	<u>Description</u>
Malware (Malicious Software)	Malware is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server or computer network. Malware is the most common cyber tactic. In fact, nearly all other TTPs are designed to gain access to an information system for the purpose of inserting a form of malware. Malware can take many forms to include rootkit, Trojan Horse, spyware, adware, virus, and worm. ⁷²
Denial of Service (DoS) and Distributed Denial of Service (DDoS)	Sending malformed packets to a targeted system in order to saturate and ultimately exhaust the target's network bandwidth or computing resources. The DDoS is the logical extension of DoS attack. DDoS employs several (up to thousands) computers to saturate and exhaust enterprise servers until the system(s) or services, such as a web server, no longer function. ⁷³
Social Engineering	Employs behavior science and manipulation to convince users to provide unauthorized access to information systems. Users often unknowingly reveal sensitive information necessary to carry out specific actions. Users are routine targets for information gathering and often referred to as the weakest link in computer security. ⁷⁴
Phishing	A form of social engineering in which the hacker attempts to acquire sensitive information such as username and passwords by masquerading as a trustworthy entity in an electronic communication. ⁷⁵
Backdoor	A covert means to bypass security controls by inserting unauthorized access into procured software or hardware. Tight supply chain management standards are needed to avoid the presence of backdoors during server and application life cycle development and acquisition. ⁷⁶
Eavesdropping and War Driving	Unauthorized network sniffers, often while driving an automobile, eavesdrop on wireless connections to gain and exploit critical information and/or passwords. ⁷⁷
Pharming	An attack that redirects traffic from an authorized website to an unauthorized website. Pharming uses a variety of methods to redirect a user to a spoofed website. ⁷⁸

Table 2: Hacker Tactics, Techniques and Procedures

⁷² U.S Army Signal Center Fort Gordon, GA, "Information Assurance Fundamentals Training: Subheading Network/Hacker Threats," U.S Army, <https://ia.signal.army.mil/IAF/default.asp> (accessed December 18, 2012).

⁷³ Harris, CISSP: All in One Exam Guide, 1014.

⁷⁴ Ibid., 61.

⁷⁵ Ibid.

⁷⁶ U.S. Army Signal Center Fort Gordon, GA, "Information Assurance Fundamentals Training."

⁷⁷ Ibid.

⁷⁸ Ibid.

Finally, cyber tactics produce multiple information system effects that facilitate the actor's ability to deceive, disrupt or destroy software. Confidentiality, Integrity, and Availability (CIA Triad) represent the three traditional pillars of the Information Security. All security controls and safeguards are implemented to address vulnerability among one or more of these principles. Cybersecurity practitioners measure all cyber risks, threats, and vulnerabilities against their potential for compromise by one or all of the CIA principles.⁷⁹ The VERIS incident framework adopts the "Parkerian Hexad," which pairs three additional effects with the three traditional effects.⁸⁰ The pairings result in a complete and granular framework that reduces the complexity and difficulty of describing cyber effects. Possession, authenticity, and utility are paired with confidentiality, integrity and availability respectively.⁸¹ Table three, Cyber Attack Effects, examines the combinations of a hacker's desired cyber attack effects.

⁷⁹ Harris, CISSP: All in One Exam Guide, 59-60.

⁸⁰ Adam Beaument and David Pym, "Structured Systems Economics for Security Management" (Ninth Workshop on the Economics of Information Security (WEIS), Harvard University, June 7-8, 2010), 2.

⁸¹ The extended framework is sometimes referred to as the "Parkerian Hexad," after the designer, Donn Parker.

Effect	Description
<u>Confidentiality/Possession</u>	
Confidentiality	Ensures that the necessary level of secrecy is enforced at each stage of data processing and prevents unauthorized disclosure. The necessary level of secrecy should prevail while data resides on enterprise systems, user devices, and transmitting the network. ⁸²
Possession	The degree to which the system owner retains possession and control of information or information systems and has the ability to prove such control. The absence of possession or control indicates the system owner lacks exclusive custody and control over information. The concept of endangerment (exposure to potential compromise) is associated with this attribute whereas actual observation or disclosure of data falls under confidentiality. ⁸³
<u>Integrity/Authenticity</u>	
Integrity	The assurance of accuracy and the prevention of unauthorized modification to information and information systems. The protection of information systems and networks from outside interference and contamination is essential to the integrity of stored information. ⁸⁴
Authenticity	The validity, conformance, correspondence to intent, and genuineness of the information asset or data. Loss of authenticity includes misrepresentation, repudiation, and/or misappropriation. Information must be valid, genuine, and must conform to its designed intent. ⁸⁵
<u>Availability/Utility</u>	
Availability	Ensures timely access to data and resources to authorized individuals. Systems and networks should provide adequate capacity so that productivity is not negatively affected. Single points of failure should be avoided, back up measures taken, and the negative effects from environmental factors prevented. Availability is essentially “Up-Time” of a system. ⁸⁶
Utility	The usefulness or fitness of the asset (or information) for its intended purpose. Loss of utility includes conversion to a less useable or unintended form. Utility is distinguished from availability in that the data is still present but no longer as useable or fit for its intended purpose. ⁸⁷

Table 3: Cyber Attack Effects

⁸² Beautenent and Pym, "Structured Systems Economics for Security Management," 60-61.

⁸³ Verizon Business, "Verizon Enterprise Risk and Information Sharing (VERIS) Community," Verizon Business, <http://www.veriscommunity.net/doku.php?id=attributes> (accessed September 21, 2012).

⁸⁴ Harris, CISSP: All in One Exam Guide, 60.

⁸⁵ Verizon Business, Verizon Enterprise Risk and Information Sharing (VERIS) Community.

⁸⁶ Harris, CISSP: All in One Exam Guide, 59-60.

⁸⁷ Verizon Business, Verizon Enterprise Risk and Information Sharing (VERIS) Community.

The multi-dimensional cyber threat is complex and requires an understanding of cyber actors, tactics, and desired effects. The range of motives should point cybersecurity practitioners to focus on the most likely cyber tactics. However, cyber strategists and policy makers must calculate the potential effects of the most dangerous scenarios capable of rivaling a national disaster. Stuxnet is that type of catastrophic event. Although Stuxnet has yet to galvanize the national will, the malicious code is certainly a precursor to impending events.

Case Study: Stuxnet

I know that when people think of cybersecurity today, they worry about hackers and criminals, who prowl the Internet, steal people's identities, steal sensitive business information, [and] steal even national security secrets. Those threats are real and they exist today. But the even greater danger – the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber terrorist attack could virtually paralyze this nation.
– Sec. of Defense Leon Panetta, October 2012.⁸⁸

Scientific research concludes that Stuxnet's primary objective was to sabotage Iranian uranium enrichment processes by reprogramming centrifuges to operate outside of specified speed boundaries.⁸⁹ Whether Stuxnet becomes a barely noticed prodromal event to a future catastrophic crisis or a watershed Sputnik moment that spurs the national will toward innovative solutions is yet to be determined. However, this Stuxnet case study reveals the potential dangers to the United States' critical infrastructure information environments. Stuxnet, a self-replicating computer virus, surgically targeted the Iranian

⁸⁸ Leon Panetta, *Remarks by Secretary of Defense Leon Panetta to the Business Executives for National Security* (Washington, DC: Office of the Secretary of Defense, October 11, 2012), <http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5136>; (accessed November 19, 2012).

⁸⁹ Eric Chien, Nicolas Falliere, and Liam Murchu, *W32. Stuxnet Dossier: Version 1.4* (Cupertino, CA: Symantec Corporation, 2011), 47.

nuclear program and delayed their uranium enrichment capability.⁹⁰ Stuxnet is the first clear evidence of an ultra-sophisticated malware directed against a nation state's industrial infrastructure.⁹¹ Symantec, a global leader in software security, concluded its comprehensive report on Stuxnet by stating, "The real-world implications of Stuxnet are beyond any threat we have seen in the past. Despite the exciting challenge in reverse engineering Stuxnet and understanding its purpose, Stuxnet is the type of threat we hope to never see again."⁹² This section presents a case study examination of the Stuxnet cyber attack in order to illuminate the rising and genuine threat to critical infrastructures. Stuxnet executed four major technological functions: (1) gain physical access to valued information systems, (2) operate nearly undetected, (3) exploit Microsoft Windows Operating System (OS) vulnerabilities, and (4) disrupt uranium program logic controllers (PLC).⁹³

First, traditional information security access control measures proved ineffective against a sophisticated and determined attacker. Stuxnet's perpetrator introduced at least three universal serial bus (USB) devices, containing three iteratively lethal versions, into five Iranian industrial environments over a ten month period.⁹⁴ Industrial computing environments typically air-gap or physically separate essential computing systems from

⁹⁰Chien, Falliere, and Murchu, *W32. Stuxnet Dossier: Version 1.4*, 11.

⁹¹ "The Stuxnet Worm," *Chemical Engineering* 118, no. 6 (June 2011), <http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/883164000?accountid=12686> (accessed November 19, 2013).

⁹² Chien, Falliere, and Murchu, *W32. Stuxnet Dossier: Version 1.4*, 55.

⁹³ Michael, "A Declaration of Cyberwar."

PLC: a small computer that controls industrial machinery. PLCs regulate the critical functions of modern industrial environments. PLCs are used for countless computer operated industrial purposes to include, control pressure within water pipes, spinning speeds of uranium centrifuges, and timing of traffic lights.

⁹⁴ Michael, "A Declaration of Cyberwar."

the global Internet.⁹⁵ However, as economies globalize, air-gapping industrial systems from the Internet has become extremely inconvenient to maintain. Software vendors reduce costs and improve just in time software maintenance by replacing traditional courier methods with online software downloads. Industrial factories must connect critical systems to the Internet in order to take advantage of faster supply chain management processes.⁹⁶ Global Internet access provides the most convenient and cost effective method to obtain downloadable software patches.⁹⁷ Introducing infected universal serial bus (USB) storage devices, often coupled with social engineering tactics, is an effective strategy to infiltrate air-gapped systems. On three occasions, between June 2009 and May 2010, Stuxnet took direct aim at specific organizations within the Iranian industrial infrastructure.⁹⁸ However, June 17, 2010 marks the date of Stuxnet's public discovery.⁹⁹ Therefore, Stuxnet operated undetected through thousands of computers for an entire year before a small Belarus cybersecurity firm uncovered the zero day malicious code.¹⁰⁰ Administrative, physical, and technical access control measures failed to prevent

⁹⁵ Steve Cunningham, "Cyber Security for Industrial Control Systems," *Power Engineering* 15, no. 11 (June 2011):142, <http://search.proquest.com.ezproxy6.ndu.edu/docview/910071964?accountid=12686> (accessed February 23, 2013).

⁹⁶ Ibid.

⁹⁷ Ibid.

⁹⁸ John Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says," *New York Times*, February 13, 2011, <http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/851394210?accountid=12686> (accessed November 20, 2012).

⁹⁹ "A Cyber-Missile Aimed at Iran?" *The Economist (Online)*, September 24, 2010, <http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/850836748?accountid=12686> (accessed November 20, 2012).

VirusBlookAda, a small Belarus cybersecurity firm, was the first to discover the malicious code within their Iranian client's computing system.

¹⁰⁰ Chien, Falliere, and Murchu, *W32. Stuxnet Dossier: Version 1.4*, 4-15.

Stuxnet's propagation into Iranian digital networks.¹⁰¹ Once inside the industrial computing environment, Stuxnet spread across the local area network (LAN) on a self-guided seek and disrupt mission.

Second, Stuxnet contained an unprecedented technological capability to conceal its presence. Malicious code often contains forged digital signatures to deceive authentication servers and host computers into a trust relationship. However, Stuxnet contained two *authentic* digital signatures that allowed the worm instant anonymity.¹⁰² The authentic digital signatures provided Stuxnet with unquestioned and unimpeded access to Iranian industrial intranet. No other malicious code has ever employed even one authentic digital signature.¹⁰³ The authentic digital certificates established trust relationships with disparate, but connected, computer systems. One computing system monitored and displayed centrifuge levels while another computing system directed actual industrial functions.

Third, Stuxnet exploited the Microsoft Windows Operating System within the supervisory control and data acquisition (SCADA) system that allowed computers to accurately monitor and display centrifuge performance.¹⁰⁴ In the weeks following Stuxnet's discovery, Microsoft collaborated with software giants, Kaspersky and Symantec, to develop mitigation and clean up strategies. The security teams' analysis

¹⁰¹ "The Stuxnet Worm."

¹⁰² "Safeguarding Critical Infrastructure from the Next Stuxnet." *Network World (Online)*, April 27, 2011, <http://search.proquest.com.ezproxy6.ndu.edu/docview/864208818?accountid=12686>. (accessed November 20, 2012).

¹⁰³ Ibid.

¹⁰⁴ Gregg Keizer, "Is Stuxnet the Best Malware Ever?" *InfoWorld*, <http://www.infoworld.com/print/137598>. (accessed September 14, 2012).

revealed Stuxnet exploited an unprecedented four zero day vulnerabilities.¹⁰⁵ Most information computer security firms view the exploitation of one zero day vulnerability the work of an expert hacker.¹⁰⁶ Stuxnet caused monitoring computers to display inaccurate centrifuge speed levels, while other Stuxnet functions worked to disrupt centrifuge critical functions. Stuxnet simultaneously prevented monitoring systems from accurately reporting abnormal centrifuge levels.¹⁰⁷

Fourth, Stuxnet reprogrammed Iranian uranium centrifuges to operate beyond specified speed boundaries.¹⁰⁸ Stuxnet contained over seventy software instructions, termed function blocks, capable of altering a programmable logic controller's (PLC) intended function.¹⁰⁹ Programmable logic controllers are specialized computers that control industrial machinery and regulate critical industrial functions.¹¹⁰ Stuxnet included rogue function blocks designed to supplant the genuine function blocks contained within a *specific* Siemens model PLC, the Siemens S57. The Iranian nuclear facility, near Natanz, widely employed Siemens S57s to control speed rates of uranium centrifuges.¹¹¹ In 2009, well before Stuxnet's public discovery, international inspectors discovered roughly a thousand Natanz gas centrifuges were inoperable.¹¹² Additionally,

¹⁰⁵ Michael, "A Declaration of Cyberwar."

¹⁰⁶ Ibid.

¹⁰⁷ Ibid.

¹⁰⁸ Chien, Falliere, and Murchu, W32. Stuxnet Dossier: Version 1.4, 43.

¹⁰⁹ "The Stuxnet Worm."

¹¹⁰ Ibid.

PLCs are used for countless computer operated industrial purposes to include control pressure within water pipes, spinning speeds of uranium centrifuges, and timing of traffic lights.

¹¹¹ Ibid.

¹¹² Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says."

the Symantec report concludes that nearly seventy percent of the one hundred thousand infected computer systems occurred within Iranian industrial environments.¹¹³

The Stuxnet worm maintained surreptitious and repudiative characteristics while achieving the disruptive and purposeful effects of a cruise missile. Stuxnet is the first worm to exploit four zero-day vulnerabilities, contain two authentic digital certificates, and inject code into industrial control systems while concealing data from monitoring stations.¹¹⁴ Although Stuxnet broke all the norms for malicious code, it has yet to thrust national policy makers or the American public into intellectual crisis. However, Secretary of Defense Leon Panetta's tone and tenor during a 2012 speech relayed the strategic implications of Stuxnet when he stated, "As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East."¹¹⁵ Stuxnet is of such complexity, not unlike nuclear weapons, that few actors possess the resources necessary to produce a similar threat.¹¹⁶ By comparison, Conficker, malware's previous heavyweight champion, contained software code one-twentieth the size and lacked Stuxnet's functional complexity. However, the costs associated with advanced technologies continue to lower over time and the implications of a Stuxnet-like attack against an electrical grid or water purification systems are too catastrophic to continue along the natural science path of the

¹¹³ Chien, Falliere, and Murchu, *W32. Stuxnet Dossier: Version 1.4*, 7.

¹¹⁴ *Ibid.*

¹¹⁵ Panetta, Remarks by Secretary of Defense Leon Panetta.

¹¹⁶ Michael, "A Declaration of Cyberwar."

past twenty years. As costs lower, global actors will seek to replicate Stuxnet in both purpose and complexity.¹¹⁷

¹¹⁷ Many investigative journals and security analysts point to the United States and/or Israel as the Stuxnet creator. However, the Symantec report indicates that only a state sponsored agency is capable of developing such complex malicious code, but the report stops short of confidently implicating an attacker.

CHAPTER 2: CYBER SPACE POLICY REVIEW

This chapter examines nearly two decades of cybersecurity policy. The policy research reveals two flawed theories, first established by the Clinton Administration, that continue to drive the United States cybersecurity strategy. The United States cybersecurity paradigm rests upon the Incremental Progress theory and the Self-Regulation theory. Three principle beliefs underpin the theories that shape United States cybersecurity debate. The beliefs that (1) voluntary information sharing between industry and government is more effective than mandated information sharing, (2) economic market forces inherently drive private owners of critical infrastructures toward cybersecurity best practices, and (3) incremental cybersecurity improvement is more effective than revolutionary changes.¹

The foundational cybersecurity principles are reminiscent of the first century Ptolemaic theory of astronomy that purported the Earth as both stationary and the center of the universe. Initially, the Ptolemaic theory successfully predicted the positioning of known planetary objects.² However, as civilizations advanced and observation tools improved, the Ptolemaic theory failed to resolve the increasing quantity of orbital anomalies. By the sixteenth century, a contentious intellectual crisis resulted in the Copernican theory of astronomy that codified the sun as the center of the universe.³ Likewise, successive United States Presidential Administrations cling to an outdated paradigm that fails to resolve the challenges within an increasingly dangerous

¹ President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting Americas Infrastructure* (Washington, DC: Government Printing Office, October 1997), 23.

² Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago: The University of Chicago Press, 1962), 68.

³ Kuhn, *The Structure of Scientific Revolutions*, 69.

cybersecurity environment. However, the United States does not have the luxury of waiting fifteen hundred years to abandon its flawed cybersecurity paradigm.

This chapter divides the historical examination of cybersecurity of critical infrastructure into three historical periods: The Second Clinton Administration (1996-2000), The Bush Administrations (2001-2008), and The First Obama Administration (2009-2012). The review examines Presidential Directives, Executive Orders, policy documents and Congressional legislation.

The Second Clinton Administration (1996-2000)

The Information Age ushered a new wealth system of globalization that forced United States' policy makers to evaluate emerging threats to national security.⁴ Although the United States' policy for securing information systems dates back to twentieth century radiotelegraphs, sustained and formal emphasis in the modern Information Age began in 1996 with the issuance of Presidential Executive Order 13010.⁵ On July 15, 1996, Presidential Executive Order 13010 codified new language within the national security environment, initiated the United States cybersecurity of critical infrastructure paradigm, and created the President's Commission on Critical Infrastructure Protection. Presidential Executive Order 13010 formally acknowledged the reality that the preponderance of national critical infrastructure ownership resides within the commercial sector. As of 2012, private sector ownership of United States' critical infrastructure

⁴ Tom Leithauser, "CRS Report Paints Complex Picture of Cybersecurity Policy Landscape," *Cybersecurity Policy Report* (December 2011): 1, <http://search.proquest.com.ezproxy6.ndu.edu/docview/920195648?accountid=12686> (accessed February 24, 2013).

⁵ Executive Order no. 13010, "Critical Infrastructure Protection," *Federal Register* 61, no. 138, title 3 (July 15, 1996), <http://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf> (accessed October 27, 2012).

exceeded eighty percent.⁶ Privately owned critical infrastructures, to include electrical grids, oil and gas pipelines, and water treatment facilities, are national capabilities that underpin the United States' economy, social structures, and national defense. Executive Order 13010 was the first national policy document to define cyber threats within the context of national critical infrastructure. Executive Order 13010 definition of critical infrastructure is listed below:

Critical infrastructures are certain national infrastructures so vital that their incapacity or destruction would have a *debilitating impact on the defense or economic security* of the United States.

These critical infrastructures include telecommunications, electrical power systems, gas and oil storage, transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Because many of these critical infrastructures are *owned and operated by the private sector*, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.⁷

Presidential Executive Order 13010 established the President's Commission on Critical Infrastructure Protection to accomplish the following tasks:

1. Assess the scope and nature of vulnerabilities and threats to critical infrastructures.
2. Determine the legal and policy issues contained within efforts to protect critical infrastructures; How can such issues be addressed?
3. Recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures *from physical and cyber threats* and assure their continued operation.

⁶ Telecommunications Industry Association, "Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain," Telecommunications Industry Association, <http://tiaonline.org/policy/securing-network-cybersecurity-recommendations-critical-infrastructure-and-global-supply> (accessed January 18, 2012).

⁷ Executive Order no. 13010, "Critical Infrastructure Protection." (*emphasis added*)

4. Propose statutory or regulatory changes necessary to effect the strategy's recommendation; and produce reports and recommendations.

Armed with specified tasks, the Commission established a national cybersecurity framework that impeded efforts to secure information systems within critical infrastructures nearly twenty years later.

In 1997, the Commission issued its report entitled, *Critical Foundations: Protecting America's Infrastructures*. The late 1990s serve as the historical backdrop for the Clinton Administration policy report. During this period, the private sector controlled the majority of critical infrastructures, information systems dependency grew exponentially, and the borderless networked environment created tremendous economic opportunities. *Critical Foundations* is the first major policy document to address critical infrastructure protection (CIP).⁸ Despite the explicit task from Presidential Executive Order 13010 to focus on physical and cyber threats, the fifteen month strategic analysis of national infrastructure resulted in a one hundred ninety-two page report that dedicates less than five pages to the physical threats against critical infrastructure. The omission of physical threats from the final report underscores the emerging digital environment marked by the late nineties. *Critical Foundations* asserts that the physical security mindset "that served us so well in the past, offer little protection from the cyber threat."⁹ At initial glance, *Critical Foundations* depicts an awareness of a changing strategic environment and subsequent requirement for critical and creative thinking to solve

⁸ John McCarthy et al., "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 1st ed. (Dulles, VA: Potomac Books, 2009), 544.

⁹ President's Commission on Critical Infrastructure Protection, *Critical Foundations*, vii.

twenty-first century challenges. The Commission boldly begins the report declaring that the presence of information security vulnerabilities within privately owned critical infrastructures threatens to jeopardize national security in a manner that requires innovative thinking.¹⁰ However, *Critical Foundations* presents a business case and strategic plan that fails to invoke new thinking, places responsibility for public trust of critical infrastructure on market forces, and pursues an Industrial Age physical security mindset.

The Commission adopted planning precepts to guide their analysis of critical infrastructure protection. The Commission's planning guideposts restrict critical and creative thinking required to produce strategies consistent with its bold ambitions. The Commission's planning guidelines led to misguided solutions that impede the cybersecurity of critical infrastructures. Since the late nineties, policy makers routinely invoke the logic expressed within *Critical Foundations* to criticize divergent ideas resembling those expressed by the Cybersecurity Act of 2012 and this thesis. Below are the Commission's self-imposed planning guidelines (Appendix 1 depicts the Commission's Seven Point Strategy):

¹⁰ Ibid.

The Commission's Planning Guidance

Build on that which exists.

It will be easier and faster to implement, more effective, and more likely to be accepted than creating something new.

Practice continuous improvement.

Take action in affordable increments. There is no “magic bullet” solution. Aim not only to protect the infrastructures, but also to enhance them.

Coordinate security with maintenance and upgrades.

Security should be incorporated in planned maintenance and scheduled upgrades.

Depend on voluntary cooperation.

Partnerships between industry and government will be more effective and efficient than legislative regulation.

Start with the owners and operators.

They have a strong economic state in protecting their assets and maximizing customer satisfaction. They understand the infrastructures and have experience in responding to outages.

Minimize changes to government oversight and regulation.

Several of the infrastructures have a long history of government regulation, with a clear legislative mandate and a record of success. We consciously avoided proposing significant changes in regulation.

Promote government leadership by example.

Government-owned facilities should be among the first to adopt best practices, active risk management, and improved security planning.¹¹

Three of the planning guidelines produce what this author terms the Incremental Progress theory. The Commission limited its potential solutions by viewing the problem through the collective lens of (1) building on what exists, (2) practicing continuous improvement, and (3) coordinating security with maintenance and upgrades. Since the publishing of *Critical Foundations*, the United States cybersecurity policies adopt natural science strategies devoid of game changing possibilities. Commonly accepted lessons

¹¹ President's Commission on Critical Infrastructure Protection, *Critical Foundations*, 23.

from the Stuxnet attack include banning the presence of USB devices and frequent replacement of hardware and software within the industrial information environments.¹² However, these tactical approaches are inefficient, expensive and ineffective. At best, such efforts are short term procedures capable of delaying an adversary for a limited period of time. The United States must simultaneously execute short-term mitigation procedures while aggressively pursuing long term strategic solutions. Cybersecurity in the Information Age requires a revolutionary shift. Unfortunately, the Incremental Progress theory continues to dominate the United States cybersecurity policy development processes.

Three additional planning guidelines catalyzed what this author titles the Self-Regulation theory. The Self-Regulation theory stems from the notions that cybersecurity of critical infrastructure is best executed when (1) private sector infrastructure owners voluntarily collaborate with the government cybersecurity efforts and that (2) the economic marketplace inherently drives owners toward cybersecurity best practices. Since the publishing of *Critical Foundations*, the United States cybersecurity policies consistently denounce regulatory enforcement or mandatory oversight over privately owned critical infrastructure. In 2013, Senator Jay Rockefeller (D-WV) sought cybersecurity legislation input from Fortune 500 CEOs. The results indicate that while the private sector welcomes access to government cyber threat data, CEOs oppose the concept of a mandated two-way relationship.¹³ The Chamber of Commerce successfully

¹² Deborah L. Wheeler, "Understanding Cyber Threats." in *Cybersecurity: Public Sector Threats and Responses*, ed. by Kim Andreasson, 1st ed. (Boca Raton, FL: CRC Press, 2012), 41.

¹³ J. N. Hoover, "CEOs Voice Support for Cyber Legislation, with Caveats," Information Week, <http://www.informationweek.com/government/policy/ceos-voice-support-for-cyber-legislation/240147638?queryText=cybersecurity+act+of+2012> (accessed September 21, 2012).

lobbied to emasculate the Cybersecurity Act of 2012, the most promising cybersecurity bill of the 112th Congress, by stripping directed two-way information sharing and federal oversight components from its language.¹⁴ Lobbyist, CEOs, and government officials continue to purport the Self-Regulation theory as a proven concept for national cybersecurity.

In response to the *Critical Foundations* report, the Clinton Administration issued Presidential Decision Directive 63 (PDD-63) for the explicit purpose of producing a “workable and innovative framework for critical infrastructure protection.”¹⁵ Below is the cybersecurity framework as outlined by PDD-63:

Immediately establish a national center to warn of and respond to attacks;

Ensure the capability to protect critical infrastructures from intentional acts by 2003.

Addresses cyber and physical infrastructure vulnerabilities within the Federal government by requiring each department and agency to work to reduce its exposure to new threats;

Requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained;

Seeks the *voluntary participation* of private industry to meet common goals for protecting our critical systems through *public-private partnerships*;

Protect privacy rights and *utilize market forces*. *It is meant to strengthen and protect the nation's economic power, not to stifle it*;

Seek full participation and input from the Congress.¹⁶

¹⁴ Ibid.

¹⁵ U.S. Presidential Decision Directive 63, "Protecting America's Critical Infrastructure," (May 22, 1998), <http://www.fas.org/irp/offdocs/pdd-63.htm> (accessed October 27, 2012).

¹⁶ Ibid. (*emphasis added*)

The Self-Regulation and Incremental Progress theories influence every cybersecurity debate and policy to include those created by the Bush and Obama Administrations. These flawed theories negatively influence Presidential and Congressional efforts to secure critical infrastructure.

The Bush Administration (2001-2008)

The terrorist attacks on September 11, 2001 spawned three legislative codes that affected the nation's approach to cybersecurity of critical infrastructure: USA PATRIOT ACT, the Homeland Security Act of 2002, and the Federal Information Security Management Act of 2002 (FISMA). While neither the Uniting Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001 (USA PATRIOT Act) nor the Homeland Security Act of 2002 are cybersecurity centric, both add insight into the United States' paradigm for the cybersecurity of critical infrastructure. Section 217 of the USA PATRIOT Act includes a provision that allows private companies the voluntarily option to authorize law enforcement to intercept electronic communication.¹⁷ The Homeland Security Act of 2002 (HSA) created the Department of Homeland Security and consolidated many operational cybersecurity responsibilities under the purview of the newest cabinet level agency.¹⁸ In December 2003, Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection* designated the Department of Homeland Security as the lead agency for Information Technology and Communications sectors, with the specific responsibility to share threat information, help assess vulnerabilities,

¹⁷ Daniel Castro, "U.S. Federal Cybersecurity Policy," in *Cybersecurity: Public Sector Threats and Responses*, ed. by Kim Andreasson. 1st ed. (Boca Raton, FL: CRC Press, 2012), 127-58.

¹⁸ Ibid.

encourage appropriate protective action, and develop contingency plans.¹⁹ In 2010, the Department of Homeland Security became the lead agency for the national implementation of the Federal Information Security Management Act of 2002.²⁰ While other federal agencies maintain significant cybersecurity responsibilities, the DHS is the lead agency for the protection of critical infrastructure.²¹

The Federal Information Security Management Act of 2002

In 2002, the 107th Congress passed the Federal Information Security Management Act (FISMA) as Title III of the E-Government Act of 2002 in response to growing threats within cyber space.²² The Federal Information Security Management Act of 2002 consolidated overlapping responsibilities and eliminated obsolete mandates contained within the Paperwork Reduction Act of 1980, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, and the Computer Security Act of 1987.²³ Congress enacted FISMA, the nation's most comprehensive cybersecurity legislation, to establish information security protections commensurate with risks to government

¹⁹ U.S. President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington DC: Government Printing Office, May 2009), www.whitehouse.gov/assets/documents/cyberspace_policy_review_final.pdf (accessed August 11, 2012), 4.

²⁰ Executive Office of the President, Memo to the Heads of Executive Departments and Agencies, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, April 21, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf (accessed September 21, 2012).

²¹ Ibid.

²² National Institute of Standards and Technology, "Security Management and Assurance: FISMA Overview," U.S. Department of Commerce, <http://csrc.nist.gov/groups/SMA/fisma/overview.html> (accessed January 18, 2012).

²³ Daniel White, "The Federal Information Security Management Act of 2002: A Potemkin Village," *Fordham Law Review* 79, no. 1 (October 2010): 369, <http://fordhamlawreview.org/articles/the-federal-information-security-management-act-of-2002-a-potemkin-village> (accessed October 4, 2012).

information systems.²⁴ While the DHS is the lead agency for implementation and compliance with FISMA, the Office of Management and Budget (OMB) ensures FISMA compliance, submits an annual report to Congress, and maintains punitive IT budgetary authority over federal agencies.²⁵ Additionally, each agency Inspector General submits an annual best practice security control evaluation to Congress.²⁶ The National Institute of Science and Technology (NIST) authors FISMA implementation strategies. Although private owners of infrastructure are not bound by FISMA, the law's construct provides an applicable window into how the United States might regulate privately owned and operated critical infrastructures. The remainder of this section examines FISMA's construct.

The National Institute of Science and Technology (NIST) risk-management framework (RMF) is the centerpiece of the federal government's cybersecurity implementation approach. In 2010, the FISMA compliance model transitioned from a static Certification and Accreditation (C&A) process into a continuous Risk Management Framework (RMF).²⁷ The C&A process is best described as a static snapshot in time inspection where results become obsolete quickly. The Certification and Accreditation compliance methodology steers federal agency information security efforts toward strict regulatory compliance often at the detriment of effective cybersecurity best practices.

²⁴ Office of Management and Budget, FY 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002 (Washington DC: Government Printing Office, March 2012), 6.

²⁵ Ibid.

FISMA compliance is not applicable to national security related information security within the federal government (DoD and CIA).

²⁶ Office of Management and Budget, *FY 2011 Report to Congress on FISMA*.

²⁷ National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Rev. ed. (Washington DC: Government Printing Office, February 2010), 1.

For example, the FY2008 Office of Management and Budget FISMA implementation report provided a Certification and Accreditation grade of satisfactory or higher to ninety-two percent of federal agencies.²⁸ However, for this same time period, a GAO report stated that the same agencies “did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information.”²⁹ Conversely, the RMF is a six-phased life-cycle management process designed to assess and mitigate an information systems’ vulnerabilities from acquisition to retirement.

The most accurate assessment of the Act’s ability to improve cybersecurity is one of unrealized potential. In 2011, the GAO reported a 650% increase of information security incidents directed against federal agencies between 2006 and 2011.³⁰ However, incident rates are not necessarily accurate measurements of cybersecurity performance.³¹ CIOs and IT managers often discover previously concealed cyber vulnerabilities and intrusions after introducing improved intrusion detection systems and intrusion prevention systems (IDS/IPS) to the information environment. Effective IDS/IPS often

²⁸ J. N. Hoover, "Cybersecurity Balancing Act," Information Week, <http://www.informationweek.com/security/government/cybersecurity-balancing-act/217100126> (accessed September 21, 2012).

²⁹ Government Accounting Office, *Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies*, by Gregory Whilshuen (Washington DC: Government Printing Office, 2008), 3.

³⁰ Government Accounting Office, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, by Gregory Whilshuen (Washington DC: Government Printing Office, 2011), 4.

³¹ Robert O'Harrow, "Hacking Tool Kits, Available Free Online, Fuel Growing Cyberspace Arms Race." *Washington Post*, November 13, 2013, http://www.washingtonpost.com/investigations/hacking-tool-kits-available-free-online-fuel-growing-cyberspace-arms-race/2012/11/12/1add77a4-21e6-11e2-ac85-e669876c6a24_story.html?wpisrc=emailtoafriend (accessed November 15, 2013).

The global explosion of pre-packaged malicious software occurred during the same time period (2006-present). Therefore, the gross quantity, access and execution of pre-packaged malicious code is much simpler than ever before. The computer technology skill set required to launch a cyber attack is lower than at any other point in history. This trend is expected to continue.

transforms *unknown unknowns* and *unknown knowns* into *known knowns*.³² In fact, the U.S Computer Emergency Readiness Team (US-CERT), a division of the DHS, attributes the GAO's reported growth statistics, at least in part, to improved intrusion detection procedures and technology.³³

The 2011 GAO report's most damaging conclusion is the systematic lack of information security controls across federal agencies.³⁴ FISMA requires agency Inspector Generals and the GAO, under the purview of the OMB, to conduct annual security control evaluations, determine deficiencies, and remediation actions.³⁵ The 2011 GAO report concluded that widespread information security control deficiencies within federal agencies expose information systems to "elevated risk of unauthorized use, disclosure, modification, and disruption."³⁶ The report cited systematic deficiencies across control areas to include access control, configuration management, and continuity of operations.³⁷ Specifically, among the most damaging and pervasive weaknesses are

³² Slavoj Zizek, "What Rumsfeld Doesn't Know that He Knows about Abu Ghraib," In *These Times* and the Institute for Public Affairs, <http://inthesetimes.com/article/747/> (accessed January 21, 2013), (*emphasis added*).

³³ Government Accounting Office, *Information Security: Weaknesses Continue*, 4.

³⁴ *Ibid.*, 11.

³⁵ National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework*, 42.

³⁶ Government Accounting Office, *Information Security: Weaknesses Continue*, 11.

³⁷ *Ibid.*

Government Accounting Office's information security management controls:

Access control: ensures only authorized individuals can view/read, modify or delete information.

Configuration Management Control: ensures CEO/CIO/IT management approved software or network additions, deletions or modifications are conducted to enterprise level software/hardware.

Segregation of Duties: reduces the risk that one individual (to include authorized system administrators) can independently perform inadvertent or inappropriate enterprise level configuration changes.

Continuity of Operations: Ensures a CEO/CIO approved plan to maintain some or all enterprise information functions in the case of widespread information loss. Examples: SIPRnet, Blackberry Enterprise Server, email, and collaboration sites.

the lack of continuous monitoring mechanisms and adequate identification and authentication measures.³⁸

In 2010, the Obama Administration identified three FISMA priorities, Continuous Monitoring, Trusted Internet Connections (TIC), and Federal Personal Identity Verification (PIV), designed to improve cybersecurity across the federal government. Among these priorities, continuous monitoring represents the largest potential to evolve FISMA into an effective cybersecurity regulation. The ultimate goal of continuous monitoring is to overlay each federal agency's information security environment and create a cybersecurity common operating picture (COP) that reveals seams, trends and threats.³⁹ In 2011, the OMB directed federal agencies to collect continuous monitoring and data feeds and submit results via Cyber Scope. Cyber Scope, a secure reporting software platform designed to replace unsecure email reporting, represents the first step toward continuous monitoring.⁴⁰ However, Cyber Scope does not perform actual continuous monitoring functions. Cyber Scope improves the security, timeliness, standardization of automated reporting, *not monitoring*.⁴¹ Cyber Scope's standardized reporting metrics and procedures provide increased insight into federal information security environment's data points.⁴² However, sixteen of the twenty-four major U.S. federal agencies did not monitor networks adequately for suspicious activities and were

³⁸ Ibid., 33.

³⁹ Phillip Kimmey, "FISMA, Cyberscope, and Federal IT Security," Center for Strategic and International Studies, <http://csis.org/blog/fisma-cyberscope-and-federal-it-security> (accessed January 14, 2013).

⁴⁰ Kimmey, "FISMA, Cyberscope, and Federal IT Security."

⁴¹ Ibid.

⁴² Ibid.

unable to report timely information security incidents.⁴³ Although Cyber Scope will allow the DHS to better understand vulnerabilities with the federal information environment, the vast majority of vulnerabilities will remain *unknown unknowns* until a viable continuous monitoring process is implemented. The Federal Information Security Management Act of 2002 continues to improve as an iterative process and serves as a preview of how the United States could regulate the cybersecurity of privately owned critical infrastructure.

The 2003 National Strategy to Secure Cyber Space

The Bush Administration's *2003 National Strategy to Secure Cyber Space (2003 National Strategy)* is based upon the Self-Regulation theory. The Self-Regulation theory is a pillar of the United States' cybersecurity of critical infrastructure paradigm. This paradigm is unlikely to reduce the risks of a catastrophic cyber attack. The *2003 National Strategy's* guiding principles contend that economic market inherently steer private owners of critical infrastructures toward cybersecurity best practices and that voluntary information sharing between industry and government is more effective than mandated information sharing. The *2003 National Strategy's* implementation of the Self-Regulation theory reads as follows:

Regulation and Market Forces: Federal regulation will not become a primary means of securing cyber space. Broad regulations mandating how all corporations must configure their information systems could divert more successful efforts by creating a lowest common denominator approach to cybersecurity, which evolving technology would quickly marginalize. Even worse, *such an approach could result in less secure and more homogeneous security architectures than we have now*. By law, some federal regulatory agencies already include cybersecurity

⁴³ Government Accounting Office, Information Security: Weaknesses Continue, 13.

considerations in their oversight activity. However, *the market itself is expected to provide the major impetus to improve cybersecurity.*⁴⁴

The Self-Regulation theory has not successfully withstood the realities of the information security environment. The frequency and lethality of targeted cyber attacks against United States' critical infrastructure is increasing at an alarming rate.⁴⁵ In 2011, hackers breached several United States financial institutions to include the NASDAQ Stock Market.⁴⁶ In 2012, the United States banking industry experienced a massive coordinated Distributed Denial of Service attack.⁴⁷

In 2004, CIO Magazine published a special edition article titled, "Tips from the Budget Masters."⁴⁸ The article presented IT budget management insights from industry leading Chief Information Officers (CIO). The former CIO of PNC Financial Services Group, Tim Shack, outlined PNC's approach to information technology (IT) strategic

⁴⁴ U.S. President, *The National Strategy to Secure Cyberspace* (Washington DC: Government Printing Office, February 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed October 4, 2012), 15. (*emphasis added*)

⁴⁵ House Committee on Homeland Security, Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, 112th Cong., 1st sess., June 24, 2011, 11.

⁴⁶ *Ibid.*

⁴⁷ Tracy Kitten, "Are Banks Winning the DDoS Battle?" Information Security Media Group Corporation, <http://www.bankinfosecurity.com/are-banks-winning-ddos-battle-a-5434/p-2> (accessed February 3, 2013).

The DDoS attack during the fall of 2012 impacted nearly every major U.S. financial and banking institution. The financial and banking online accessibility gold standard is 99.5%. During the fall of 2012, the accessibility rate dropped to a dismal 94.86%. As of the weekend January 13, 2012, the rate hovers at 97.21%. The impacted institutions includes: PNC Financial Services Group, BB&T, Fifth Third Bank, Bank of America, JPMorgan, Chase, Citigroup, Wells Fargo, U.S. Bancorp, CapitalOne, HSBC, Ally Bank, SunTrust Banks, Regions Financial Corp. and Zions Bancorp.

⁴⁸ Stephanie Overby, "Tips From the Budget Masters," *CIO Magazine, Special Issue*, Fall/Winter 2004, <http://books.google.com/books?id=ZwoAAAAAMBAJ&pg=PA43&lpg=PA43&dq=cio+magazine+business+case&source=bl&ots=fE8nKIDBLD&sig=1OJ5XTv57wHI8wRDd3ppbLIVGBo&hl=en&sa=X&ei=g0wNUeKbO7Dx0wGBwYHoDQ&ved=0CDAQ6AEwAA#v=onepage&q=cio%20magazine%20business%20case&f=false> (accessed February 4, 2013).

planning.⁴⁹ PNC Financial Services analyzes every potential IT strategic investments against four evaluation criteria: (1) regulatory compliance, (2) revenue generating potential, (3) expense reducing potential, and (4) competitive advantage.⁵⁰ Mr. Shack highlighted several projects, none of which targeted the firm's information security posture, as proof of the processes' strategic planning validity.⁵¹ Strategic information security investments are subjective non-revenue generating activities that companies calculate as expenses. The corporate sector's unwillingness to link strategic information security investments to valid business objectives creates underfunded cybersecurity environments. In 2012, PricewaterhouseCoopers (PwC) released its global IT security corporate investment analysis report that surveyed 9,300 CIOs, CEOs, and IT managers on their organization's preparedness against cyber attacks. The report presents four key statistics that dispel the myth of effective self-regulation.⁵²

- 8% exercise essential IT security key best practices such as delivering security reports to the CEO.
- 42% execute an effective IT security strategy
- 71% use adware and spyware detection tools (down from 83% in 2011)
- 16% conducted an inventory of essential company data in (down from 22%) to determine the organization risk level in the event of a cyber attack.

Although the *2003 Strategy to Secure Cyber Space* contends that "...the [economic] market itself is expected to provide the major impetus to improve cybersecurity," Mark Lobel, principal and primary PwC report contributor, stated that "instead of risk driving

⁴⁹ National Information Center, "The Top 50 Holding Companies," The Federal Reserve, <http://www.ffiec.gov/nicpubweb/nicweb/Top50Form.aspx> (accessed February 1, 2013).

PNC is now the twelfth largest Financial Services Institution within the United States. (\$300B)

⁵⁰ Overby, "Tips From the Budget Masters."

⁵¹ Ibid.

⁵² Ibid.

[IT] security budgets, it's [IT security measures] what can the company afford.”⁵³

Capitalist economies naturally suppress non-revenue generating investments unless an external factor, such as a federal requirement, forces its occurrence. *The 2003 National Strategy to Secure Cyber Space* is built upon the Self-Regulation theory that runs contrary to the realities within the economic marketplace.

The second Self-Regulation principle, upon which the *2003 National Strategy to Secure Cyber Space* rests, is the reliance upon voluntary public-private information sharing partnerships to secure the cyber space of critical infrastructure. The argument for voluntary public-private partnerships is grounded within the following *2003 National Strategy to Secure Cyber Space* statement:

Most critical infrastructures, and the cyber space on which they rely, are privately owned and operated. The technologies that create and support cyber space evolve rapidly from private sector and academic innovation. Government alone cannot sufficiently secure cyber space. Thus, President Bush has called for *voluntary* partnerships among government, industry, academia, and nongovernmental groups to secure and defend cyber space.⁵⁴

The 2003 National Strategy to Secure Cyber Space further supports the Self-Regulation principle of voluntary public-private partnerships by touting the United States' federalist traditions which require the private sector to “take the lead” in matters of cybersecurity.⁵⁵

The 2003 National Strategy correctly concludes that “Government alone cannot

⁵³ Joel Schectman, "PwC: Companies Trim IT Security as Budgets Stagnate," Wall Street Journal, <http://blogs.wsj.com/cio/2012/09/20/pwc-companies-trim-it-security-as-budgets-stagnate/?KEYWORDS=cybersecurity> (accessed February 1, 2013).

⁵⁴ U.S. President, *The National Strategy to Secure Cyberspace*, 2. (*emphasis added*)

⁵⁵ *Ibid.*, 14.

sufficiently secure cyber space.”⁵⁶ However, when participants to a partnership have “skin in the game” the ability to disengage from the relationship becomes difficult.

In 2011, House Republicans created a Cybersecurity Task Force in response to an acknowledged lack of cyber preparedness within the nation’s critical infrastructures.⁵⁷ The Task Force’s report acknowledged the federal government’s inherent responsibility to secure the nation’s critical infrastructure against catastrophic cyber-attacks and advocated regulatory measures.⁵⁸ The report recommends that “there may be instances where *additional* direct regulation of an industry that is already highly regulated (nuclear power, electricity, chemical plants, water treatment) may be warranted.”⁵⁹ The report formed the foundation of a comprehensive cybersecurity bill, the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PrECISE Act), that included regulating privately owned critical infrastructure.⁶⁰ However, for reasons that are unclear, but almost certainly related to the Self-Regulation theory, task force members withdrew the bill from consideration and disavowed the report they endorsed only a few months earlier.⁶¹

⁵⁶ Ibid., 2.

⁵⁷ House Republican Cybersecurity Task Force, *Recommendations of the House Republican Cybersecurity Task Force* (Washington DC: Government Printing Office, 2011), http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf (accessed February 4, 2013), 5-9.

⁵⁸ Ibid.

⁵⁹ Ibid. (*emphasis added*)

⁶⁰ Gautham Nagesh, "House Cybersecurity Bill would Establish Federal Overseer," The Hill, <http://thehill.com/blogs/hillicon-valley/technology/199929-house-members-introduce-cybersecurity-bill> (accessed February 18, 2013).

⁶¹ James A. Lewis, "Code Red," *Foreign Policy*, August 2012, http://www.foreignpolicy.com/articles/2012/08/01/code_red (accessed November 18, 2012).

The First Obama Administration (2009-2012)

The 2009 Cyber Space Policy Review

In 2009, the Obama Administration issued its signature cybersecurity policy titled, the *2009 Cyber Space Policy Review (2009 Policy Review)*. The *Cyber Space Policy Review* is the result of an executive level 60-day “clean-slate” review of United States’ cybersecurity policies and frameworks.⁶² Based on Thomas Kuhn’s theory of change, the “clean-slate” approach represents a potential conceptual recognition of prodromal symptoms that leads to an impending intellectual crisis. The United States traditional cybersecurity theories and underlying principles expose the nation’s critical infrastructure to unacceptable risk levels.

The *2009 Cyber Space Policy Review* presents two policy concepts that are divergent from the United States’ traditional approach to cybersecurity. First, the *2009 Policy Review* seeks to revamp the traditional public-private partnership relationship. Organizations often underfund non-revenue generating activities, such as strategic information security investments, due to the lack of a perceived valid business case. The *2009 Policy Review* acknowledges the private sector’s difficulty in demonstrating a compelling business case for cybersecurity investments to shareholders and boards of directors.⁶³ The *2009 Policy Review* suggests that “there are various approaches the Federal government could take to address these challenges, some of which may require changes in law and policy.”⁶⁴ During 2011 Congressional hearings on the Obama Administration’s cybersecurity legislative proposals, Larry Clinton, President/CEO of the

⁶² U.S. President, *Cyberspace Policy Review*, ii.

⁶³ *Ibid.*, 17.

⁶⁴ *Ibid.*

Internet Security Alliance, argued against changes to current legislative frameworks.⁶⁵ However, Mr. Clinton bolstered the *2009 Policy Review*'s premise for increased legislation by stating, "Some have suggested that the market has failed to produce the needed technology to address the cyber threat. That is not the case....The fact is that many companies don't see an adequate ROI to cyber investments."⁶⁶ The *2009 Policy Review* supports the adoption of legislation that creates monetary cybersecurity incentivizes for the private sector. The most promising concept includes "reduced liability in exchange for improved security or increased liability for the consequences of poor security."⁶⁷ Since liability costs are among senior management's most pressing concerns, such an approach provides corporate managers with a compelling business case for information security strategic investments. Although incentive based legislation would greatly assist the business case effort, CEOs and CIOs must communicate the monetary value of cyber vulnerabilities absent of legislative incentives.

Second, the new policy insists that the Executive Office of the President is best positioned to create synergy among federal agencies. It contends that the federal government must never abrogate its national security responsibilities to private sector balance sheets. Specifically, the *2009 Policy Review* asserts that the United States' dependence upon information and computing technologies requires leadership that is anchored to the authority of the National Security Council (NSC) and the President of the United States. In December 2009, President Obama appointed Mr. Howard Schmidt to

⁶⁵ House Committee, Examining the Homeland Security Impact, 32.

⁶⁶ Ibid.

⁶⁷ U.S. President, *Cyberspace Policy Review*, ii.

the post of Cybersecurity Coordinator.⁶⁸ Under Mr. Schmidt's leadership, the Obama Administration submitted a comprehensive legislative proposal to Congress that sought to increase federal authority over selected critical infrastructures.⁶⁹ The Senate included many of the Obama Administration's proposals within the Cybersecurity Act of 2012. Unfortunately, the Cybersecurity Act of 2012 failed to pass a Senate vote.⁷⁰ Additionally, Mr. Schmidt led the Administration's initiatives to establish Continuous Monitoring procedures, risk-based cyber management models, and Trusted Internet Connections (TIC) within the Federal Information Security Management Act. In May 2012, Mr. Michael Daniel replaced Mr. Schmidt upon his retirement from government service. The long term impacts of a national Cybersecurity Coordinator are not yet certain.

Lastly, the *2009 Policy Review* embraces the public-private partnership principle, but insists that traditional partnerships lack the organizational structures required to create meaningful results. The *2009 Policy Review* references a "diffusion of effort" within the traditional public-private principle that prevents participants from sharing ownership of the problem.⁷¹ Since 1997, Presidential Directives and Executive Orders created countless public-private information sharing committees with underwhelming results.⁷² The *2009 Policy Review* advances two concepts designed to reduce the barriers

⁶⁸ The White House, "Introducing the New Cybersecurity Coordinator," The White House, <http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator> (accessed February 9, 2013).

⁶⁹ House Committee, Examining the Homeland Security Impact, 32.

⁷⁰ Jennifer Rizzo, "Cybersecurity Deal Fails in Senate," Turner Broadcasting System, Inc., <http://www.cnn.com/2012/08/02/politics/cybersecurity-act> (accessed January 20, 2013).

⁷¹ U.S. President, *Cyberspace Policy Review*, 17.

⁷² *Ibid.*, 18.

to effective public-private partnerships. First, the traditional public-private partnership principle is based on a volunteer approach that is devoid of defined roles and responsibilities. The *2009 Policy Review* states that the federal government should provide the resources and organizational structure to existing partnerships in an effort to create accountability, optimize efforts, and develop executable response and recovery plans.⁷³ Second, the policy favors a legislative framework that tethers private sector participants to mandatory participation, clear objectives, and measurable response and recovery plans.⁷⁴ Many private sector stakeholders worry that information sharing with the DHS ultimately leads to the disclosure of egregious cyber vulnerabilities, divulgence of trade secrets, or the reduction of stock price or public trust.⁷⁵ While current laws such as the Critical Infrastructure Information Act address many private sector concerns, the potential damage from public knowledge of cyber vulnerabilities within corporate information systems may have irreversible effects on public trust or stock prices.⁷⁶ However, the Obama Administration insists that a tailored limited liability program is a necessary step to create a public-private partnership that secures national infrastructure.

Numerous United States public-private forums set out to measurably reduce the nation's risk to cyber threats to include the Critical Infrastructure Partnership Advisory Council (CIPAC), the Enduring Security Framework, the Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), the Federal Bureau of Investigation's InfraGard, U.S. Secret Service's Electronic Crimes Task Forces, the National Security Telecommunications Advisory Committee (NSTAC), the National Infrastructure Advisory Council (NIAC), the Homeland Security Advisory Council, and countless associated subcommittees and working groups.

⁷³ U.S. President, *Cyberspace Policy Review*, 18.

⁷⁴ *Ibid.*

⁷⁵ *Ibid.*, 19.

⁷⁶ *Ibid.*

CHAPTER 3: RECOMMENDATIONS

“There are no intrinsic “laws of nature” for cyber-security as there are, for example, in physics, chemistry or biology. Cyber-security is essentially an applied science that is informed by the mathematical constructs of computer science such as theory of automata, complexity, and mathematical logic”.¹ – The JASON Study Group.

This section presents the author’s cybersecurity of critical infrastructure paradigm in the form of four recommended principles:

1. Redefining Cyberspace
2. Game Changing Culture
3. Open Information Highway with Secured Exits and Assets
4. Limited Liability Legislation

Collectively, the recommended principles create a paradigm that runs contrary to traditional cybersecurity beliefs including the notions that (1) voluntary information sharing between industry and government is more effective than directed sharing, (2) economic market forces inherently drive private owners of critical infrastructures toward cybersecurity best practices, and (3) incremental cybersecurity improvement is more effective than revolutionary changes.

Recommendation: Redefining Cyberspace

Inadequate cybersecurity definitions lead United States policy makers toward the creation of ineffective cybersecurity of critical infrastructure policies. Effective cybersecurity solutions emanate only from accurate definitions of cyberspace. Both the Department of Defense and the Center for Technology and National Security Policy (CTNSP) present useful cyberspace definitions. However, the Department of Defense’s

¹ The MITRE Corporation, *Science of Cybersecurity* (Rosslyn, VA: The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2010), www.fas.org/irp/agency/dod/jason/cyber.pdf (accessed March 19, 2013).

cyberspace definition fails to identify cyberspace's purpose.² The lack of an explicit purpose within the DoD definition handicaps both the cybersecurity policy maker and practitioner's ability to link cybersecurity national interests (ends) and strategic/operational tasks (ways) to appropriate resources (means). While the CTNSP definition correctly identifies cyberspace's purpose as the ability to "create, store, modify, exchange, and exploit information," it fails to convey the essential role of software code within cyberspace.³ Software code, not the Internet, is both valued by the system owner and targeted by the cyber attacker. Software code is the genesis of every benefit, vulnerability, and threat within the information environment termed cyberspace. Therefore, an effective cyberspace definition must focus on information systems, of which the Internet is a component, that are underpinned by lines of software code. While largely accurate, neither the DoD nor the CTNSP definitions conveys the essential role of software code to cyberspace. Below is this study's recommended cyberspace definition:

The global domain within the information and communications environment consisting of communication links, hardware, and software necessary to create, modify, store, and exchange information and control computing systems; Software code is acknowledged as the central element among the three critical components that direct and control information and computing systems.

² U.S. Department of Defense, *Department of Defense Dictionary of Military Terms and Associated Terms* (Washington DC: Government Printing Office, November 2012), 77.

DoD Cyberspace Definition: The human engineered global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

³ Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 1st ed. (Dulles, VA: Potomac Books, 2009), 28.

CTNSP Cyberspace Definition: A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies.

This study's definition contains three noteworthy distinctions that are normally absent from cyberspace constructs. First, the definition identifies each essential components of cybersecurity (communication links, hardware, and software) without overemphasizing the role of the global communication links. Although responsible cybersecurity policy must address Internet security, cybersecurity is not wholly reliant upon effective Internet security. The Stuxnet Case Study provides proof that the lack of global Internet connectivity does not insulate an information system from a determined hacker. Therefore, equating cyberspace to the Internet mistakenly implies the sufficiency of Internet security as effective cybersecurity. Second, this study's definition explicitly states the purpose of cyberspace as the ability "to create, modify, store, and exchange information and/or control computing systems." Both malicious and responsible actors enter cyberspace to conduct information based functions. Understanding functionalities and purposes provides insight and context for understanding the cyber actors, tactics, and desired effects. Last and most importantly, the recommended definition presents software code as the "central element among the three critical components that directs and controls information and computing systems." As previously stated, software code, not hardware or communication links, is the most valued prize of the cyber hacker. Software represents both the brains of computing productivity and the primary source of vulnerability. Cyberspace definitions must acknowledge software's critical role within the broader context of information and computing technology systems. Equating the Internet with cyberspace undermines the nation's understanding of the information environment. In fact, the vast majority of cyber attacks are dedicated to finding, exploiting, disrupting or destroying unknown vulnerabilities, called zero day

vulnerabilities, within software.⁴ While most cybersecurity literature focuses upon Internet security, there is no defense for zero day software vulnerability.⁵ The manner in which national policy defines cyberspace drives the development of solutions that address cybersecurity challenges.

While the various information and computing functionalities serve as the purpose for human entry into cyberspace, the manner in which the United States pushes the technological envelope will determine the nation's future cybersecurity of critical infrastructure. The recommendation below seeks to recapture the United States hegemonic role at the world's leading information technology leader. The United States has been more influential in the development of cyberspace than any other. Likewise, the Defense Advanced Research Projects Agency provided the most intellectual capital into the development of cyberspace. The United States must revitalize this organization toward efforts to solve the puzzles of cybersecurity of critical infrastructure.

Recommendation: Game Changing Culture

In December 1957, the United States completed fast track production of its first space satellite, Vanguard, just two months after witnessing the technological surprise of the world's first orbiting satellite, Sputnik.⁶ The explosion of Vanguard on the launch pad spurred a demand for change from President Dwight D. Eisenhower and the nation. The changes entailed a national emphasis on science and technology and the creation of a

⁴ Jeffrey Carr, *Inside Cyber Warfare*, ed. Mike Loukides, 1st ed. (Sebastopol, CA: O'Reilly Media Incorporated, 2009), 152.

⁵ *Ibid.*, 158.

⁶ Gary Anthes, "Timeline: Sputnik and Three Decades of DARPA Hegemony," Computerworld (Online), http://www.computerworld.com/s/article/9037638/Timeline_Sputnik_and_Three_Decades_of_DARPA_Hegemony (accessed February 7, 2013).

new agency, the Advanced Research Projects Agency, with a game changing organizational culture.

The Advanced Research Projects Agency's (ARPA) mission was to "prevent technological surprise."⁷ Its organizational culture encouraged patience and tolerance for high risk/high-payoff projects.⁸ Prior to ARPA, university science programs were weak and outdated.⁹ For the first four decades of its existence, ARPA provided needed funding to scientific universities for (then) nebulous concepts to include artificial intelligence and computer chips.¹⁰ However, during the Global War on Terrorism, the agency, now called the Defense Advanced Research Projects Agency (DARPA), focused on short-term, pragmatic military objectives.¹¹ DARPA executed a strategic shift from its historical focus of nascent solutions capable of preventing technological surprise to "shovel ready" technologies that support the current fight.¹² During Congressional hearings on the National Defense Authorization Act for FY12, former DAPRA Director, Regina Dugan, testified in support of the need to return the agency to its lineage:

At DARPA we say that we must not lose the nerve for the big failure. The nerve you need for the big failure is the same as the nerve for the big success, until the moment you know which it will be. It's the exact same

⁷ Anthes, "Timeline: Sputnik and Three Decades of DARPA Hegemony."

⁸ Ibid.

⁹ Gary Anthes, "Happy Birthday Sputnik!" *Computerworld* 41, no. 44 (October 2007): 44-46, <http://search.proquest.com.ezproxy6.ndu.edu/docview/216118814?accountid=12686> (accessed March 3, 2013).

¹⁰ Ibid.

¹¹ Anthes, "Timeline: Sputnik and Three Decades of DARPA Hegemony."

¹² U. S. Congress. House Armed Services Committee, *Prepared Statement by Dr. Regina Dugan* (Washington DC: U. S. House of Representatives, 2011), http://armedservices.house.gov/index.cfm/files/serve?File_id=7ccf4551-0f9b-4212-9349-e846475c5655 (accessed January 22, 2013), 6.

nerve...we have endeavored to *revitalize* this sensibility at DARPA...the Agency's willingness to take on the big risk.¹³

The agency and its culture are responsible for the world's first distributed information network, first successful email message, first graphical user interface (GUI) computer program, and first implementation of packet switching technology into distributed networks.¹⁴ DARPA, with its brilliant personnel and unique organizational culture, initiated much of cyberspace. The United States cybersecurity paradigm should include DARPA as its lead agent for game changing and high risk/high pay off innovation. The Defense Advanced Research Projects Agency is a national asset that must recapture its role of consistently reaching *beyond* next generation technology.

In 2005, Kevin Kelley, an Arkansas high school football coach, executed a revolutionary shift from traditional coaching when he decided to stop punting the ball on fourth down.¹⁵ Coach Kelley's out of the box thinking flies in the face of the traditional American football paradigm. However, in the last three seasons Coach Kelley's team punted the ball only three times (after achieving an insurmountable lead) and reached three state semifinals, two state finals, and won the 2011 Arkansas 5A State Championship.¹⁶ Traditionalists within the collegiate and professional football coaching ranks scoff at Coach Kelley's theory. However, *the Structure of Scientific Revolutions* warns that unconventional paradigms are usually met with an unrelenting intellectual

¹³ Ibid. (*emphasis added*)

¹⁴ Anthes, "Timeline: Sputnik and Three Decades of DARPA Hegemony."

¹⁵ Gregg Eastermann, "State of High School Nation," ESPN, <http://sports.espn.go.com/espn/page2/story?page=easterbrook/071113> (accessed February 5, 2012).

¹⁶ Ibid.

barrier of resistance.¹⁷ Regardless of likely criticism, the Advanced Research Projects Agency's history and culture uniquely qualifies the agency to once again lead the nation against the growing cybersecurity problem set. The Advanced Research Projects Agency is the catalyst for much of cyberspace and it must now lead the nation in securing cyberspace. The United States and DARPA must stop punting on fourth down.

The current United States approach to cybersecurity follows an incremental and evolutionary path toward progress. While software and technology companies work frantically to introduce the next firewall appliance or reverse engineer the most recent malicious code, cyber vulnerabilities and threats outpace these incremental efforts. Recent projects at DARPA indicate a potential shift back to its lineage. The next recommendation, Open Highway and Secure Exits, highlights an emerging DARPA research concept that supports the author's contention that Internet security does not equal cybersecurity. The next recommendation reflects this reality.

Recommendation: Open Highway & Secured Exits¹⁸

The second recommended paradigm principle requires a fundamental shift in how policy makers think about cyberspace and cybersecurity. This recommendation calls for cybersecurity policy makers to direct the bulk of their focus on creating secure and resilient software systems and less focus on Internet security.

A cybersecurity policy that equates Internet security with cybersecurity is misguided. While Internet anonymity remains a hurdle to global cybersecurity,

¹⁷ Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago: The University of Chicago Press, 1962), 65.

¹⁸ In Chapter 1, this thesis analogized cyberspace as an intricate transportation systems. "Simply stated, the Internet is a networked transport path (superhighway) for varying sized information packets (cars, motorcycles, cargo vehicles) to reach desired hardware (homes, office buildings) that contain valued information and/or critical information systems (Assets: money, families, inventory) controlled by software (people)."

democratic and capitalist values flourish in the presence of an accessible, global, and interoperable communications network. Blogs, point of sale (POS) software, social media, and supply management software facilitate the success of both political activists and emerging economies. The alternative to an interoperable and globally accessible Internet is a fragmented information environment, in which nation states restrict access to advanced technologies under the guise of national security interests.¹⁹ Additionally, the Stuxnet attack illuminates critical infrastructures as viable cyber targets and the fallacy of equating Internet security with cybersecurity. The United States cybersecurity paradigm must promote secure and resilient software, while accepting a level of anonymity and risk within cyber space. Defense in depth and resilient software strategies are practical applications of this principle.

The cybersecurity paradigm demands a defense in depth philosophy to combat multiple nefarious actors and disparate attack techniques. No single administrative, physical, or technical access control measure is infallible. Therefore, the cybersecurity paradigm must include a defense in depth philosophy, in which an attacker must penetrate each aspect of a varied and layered cybersecurity strategy in order to achieve the attack objective. Multiple and varied access obstacles require increased expertise, resources, and capabilities from an attacker. Additionally, the increased levels of time and resources required to penetrate each cybersecurity layer shifts the preponderance of risks and costs from the defender to the attacker. The increased costs and risks of

¹⁹ U.S. President, *International Strategy for Cyberspace* (Washington DC: Government Printing Office, May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed August 15, 2012), 8.

exposure associated with penetrating layered cyber obstacles adhere to William Kaufmann's concept of deterrence:

Deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability actually to achieve the defense of the interest in question or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort to him.²⁰

Within the defense in depth principle, the presence of inherently secure software is the most important element. However, the design and development of inherently secure software is rare.²¹ Software developers often conclude that issuing software patches to the customer base is financially advantageous when compared to extensive security testing prior to software release.²² In fact, when quarterly earnings statements serve as the primary measuring stick, integrating inherent software security at the inception of the software life cycle development process is significantly more expensive and time-consuming.²³

Finally, this principle includes ensuring the impact of cyber attacks against critical infrastructure is limited. Future software systems must be capable of resisting and adapting to zero-day intrusions. In 2010, DAPRA's Information Innovation Office (IIO) launched the Clean-Slate Design of Resilient Adaptive Secure Host (CRASH) program

²⁰ Adam Bernstein, "Obituaries: Defense Expert William Kaufmann," *Washington Post*, December 17, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/16/AR2008121602724.html> (accessed January 15, 2013).

²¹ Seymour Goodman and Herbert Lin, *Toward a Safer and More Secure Cyberspace* (Washington DC: National Academy Press, 2007), 88.

²² David Rice, *Geekonomics: The Real Cost of Insecure Software*, (Boston, MA: Pearson Education, 2008), Kindle E-Book, Chapter 2.

²³ Ibid.

that contains the potential of reversing the asymmetrical nature of cybersecurity.²⁴ The CRASH research program explores how to design computer systems that are less vulnerable to cyber intrusions and more resilient in the event of data breach. The CRASH program includes several projects that are founded upon a single question: If the computer industry could redesign computers and software, what would it do differently?²⁵ One CRASH initiative seeks to create operating systems that emulate the resiliency and adaptability of the human immune system. The human immune system contains separate virus barriers capable of stopping known virus while other systems remember and alter cells in preparation for future attacks. A separate CRASH initiative explores a new computing architecture in which every data packet contains credentialing information. Without the necessary credentialing information, the receiving computer systems could not process the incoming data. This solution allows for an open Internet, but secures the valued information system from untrusted data packets.

Recommendation: Limited Liability Legislation

The United States requires a fundamentally different approach to cybersecurity that includes targeted legislation for private owners of critical infrastructure. Since the late 1990s, the Self-Regulation theory remains the foundation of the United States' cybersecurity paradigm. The Self-Regulation theory purports that volunteer public/private partnerships and market driven strategic investments lead to cybersecurity best practices. However, the previous fifteen years is characterized by increasing cyber related vulnerabilities and decreasing information security strategic investments. In

²⁴ John Markoff, "Killing the Computer to Save It," *New York Times*, October 30, 2012, http://www.nytimes.com/2012/10/30/science/rethinking-the-computer-at-80.html?pagewanted=all&_r=0 (accessed November 18, 2012).

²⁵ Ibid.

2009, the Wall Street Journal reported that according to national security officials “cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.”²⁶ The United States Industrial Control System Cyber Emergency Response Team (ICS-CERT) reports that the number of cyber incidents directed against U.S. critical infrastructure increased from a nearly non-existent level in 2009 to roughly two hundred in 2011. The report also indicates that water supplies are the predominate targets of attack.²⁷ The Self-Regulation theory runs contrary to both corporate strategic investment decision making and the growing cyber threat environment.

In 2011, the 112th Congress sought to create legislation to secure critical infrastructure. Some members of Congress sought to adjust the nation’s dependence on the Self-Regulation theory. The 112th Congress held roughly sixty hearings on cybersecurity and introduced over twenty significant cyber related bills.²⁸ The Cyber-Security Act of 2012 and SECURE IT Act of 2012 were the most significant efforts toward comprehensive cybersecurity legislation. Both General Keith Alexander, Commander USCYBERCOM and Director, National Security Agency, and General Martin Dempsey, Chairman of the Joint Chiefs of Staff, submitted letters to Congress urging the passage of comprehensive cybersecurity legislation.²⁹ General Alexander stated, “The cyber threat facing the Nation is real and demands immediate action. The

²⁶ Chris Brantley, "Congress Swings, Misses on Cybersecurity," IEEE, <http://www.todaysengineer.org/2012/Sep/cybersecurity.asp> (accessed March 3, 2013).

²⁷ Ibid.

²⁸ Ibid.

²⁹ Brantley, "Congress Swings, Misses on Cybersecurity."

time to act is now; we simply cannot afford further delay.”³⁰ Despite Congress’ genuine concern and recommendations from the nation’s top military advisors, Self-Regulation theorists derailed both the Cyber-Security Act of 2012 and SECURE IT Act of 2012. Congress presented a Chamber of Commerce letter to the Congressional floor just prior to the vote on the Cyber-Security Act of 2012. The letter stated that the bill “could actually impede U.S. cyber-security by shifting businesses’ resources away from implementing robust and effective security measures and toward meeting government mandates.”³¹

The lack of financial incentives dissuades the private sector from voluntarily hardening critical infrastructure information environments. In August 2010, the National Institute for Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), and over five hundred private sector participants, developed and issued the nation’s first electrical Smart Grid cybersecurity guidelines.³² However, a GAO review concluded that the FERCs lack of legislative authority hinders a complete understanding of Smart Grid vulnerabilities.³³ The GAO’s office reached five additional conclusions which point to the failure of a self-regulating voluntary approach:³⁴

- The electric industry does not have an effective mechanism for sharing information on cybersecurity.
- Consumers are not adequately informed about the benefits, costs, and risks associated with smart grid systems

³⁰ Ibid.

³¹ Ibid.

³² House Committee on Homeland Security, *Examining the Cyber Threat to Critical Infrastructure and the American Economy*, 112th Cong., 1st sess., March 16, 2011., 43.

³³ Government Accounting Office, *Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, by David Powner and David Trimble (Washington DC: Government Printing Office, 2011).

³⁴ Ibid.

- There is a lack of security features being built into certain smart grid systems.
- The electricity industry does not have metrics for evaluating cybersecurity.

The United States cybersecurity paradigm must include legislation that mandates two-way information sharing, limited liability for corporate disclosure of cyber vulnerabilities, financial incentives, and financial penalties for egregious cyber neglect. Effective legislation will avoid prescriptive standards that are easily outpaced by technological advances. Other precedents for cybersecurity standards can be found in the Consensus Audit Guidelines (CAG) developed by a consortium of federal agencies, including the National Security Agency, and several private sector organizations.³⁵ The CAG standards are both technology focused, but broad enough to encompass cybersecurity principles over an extended period of time.³⁶ The United States government maintains an inherent responsibility to protect the nation and its citizens from catastrophic attacks against the homeland. An effective cybersecurity law provides needed accountability to policy guidance. While effective legislation must not rest upon quarterly balance sheets or voluntary private/public partnerships, neither can it undermine national interests or values such as economic globalization or privacy rights. Cybersecurity legislation must include limited liability, financial incentives and penalties, and contain enough flexibility to withstand a changing technological environment.

³⁵ Government Accounting Office, Progress Being Made on Cybersecurity Guidelines, 43.

³⁶ Ibid.

CONCLUSION

The United States paradigm for the cybersecurity of critical infrastructure is flawed. For nearly two decades, the Self-Regulation and Incremental Progress theories misinformed Presidential and Congressional cybersecurity policy makers. A rapidly evolving cyber threat environment proved these theories ineffective. The technological explosion of the Information Age continues to decrease the costs and expertise required to launch increasingly complex cyber attacks. While the development of malicious code comparable to Stuxnet is currently beyond the capability and means of all except nation states, the Stuxnet attack confirms critical infrastructure as highly valued targets. Additionally, the Stuxnet attack points to a future where extremely sophisticated malicious code becomes available on the black market at costs affordable to a wider threat audience. In order to prepare for such an occurrence, the United States must undergo a cybersecurity paradigm change.

This thesis recommends three principles as part of a new United States paradigm for the cybersecurity of critical infrastructure. First, the United States must revitalize the Defense Advanced Research Projects Agency, its organizational culture, and its historical penchant to take on high risk/high payoff game changing innovation. Second, policy makers must reduce the inclination to equate cybersecurity with Internet security. Instead, policy makers must think in terms of inherently secure software systems. Lastly, the United States requires cybersecurity legislation that includes limited liability, financial incentives, as well as, financial penalties for private owners of critical infrastructure. Collectively, the new paradigm will increase the risks and costs of a cyber

attacker while reducing costs and risks to the cyber defenders of United States critical infrastructure.

APPENDIX 1: CRITICAL FOUNDATIONS SEVEN POINT STRATEGY

Critical Foundations Seven Point Strategy³⁷

Establishing the Partnership.

Promote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.

Building the Partnership.

Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.

Structuring the Partnership.

Establish national structures that will facilitate effective partnerships between the federal government, state, and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning and programs.

Report on Awareness and Education.

Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.

Leading by Example.

Initiate a series of information security management activities and related programs demonstrating government leadership.

Legal Initiatives.

Sponsor legislation to increase effectiveness of federal infrastructure assurance and protection efforts.

Research and Development.

Increase investment in infrastructure assurance research from \$250 million to \$500 million in FY99, with incremental increases over a five-year period to \$1 billion in FY04.

³⁷ President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting Americas Infrastructure* (Washington, DC: Government Printing Office, October 1997), v.

BIBLIOGRAPHY

- "A Cyber-Missile Aimed at Iran?" *The Economist (Online)*. September 24, 2010.
<http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/850836748?accountid=12686> (accessed November 20, 2012).
- "Safeguarding Critical Infrastructure from the Next Stuxnet." *Network World (Online)*. April 27, 2011.
<http://search.proquest.com.ezproxy6.ndu.edu/docview/864208818?accountid=12686>.
(accessed November 20, 2012).
- "The Stuxnet Worm." *Chemical Engineering* 118, no. 6 (June 2011).
<http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/883164000?accountid=12686> (accessed November 19, 2013).
- Abatte, Janet Ellen. "From ARPANet to Internet: A History of APRA-Sponsored Computer Networks, 1966-1988." PhD diss., University of Pennsylvania, 1994.
<http://search.proquest.com.ezproxy6.ndu.edu/docview/304104775?accountid=12686>
(accessed March 28, 2013).
- Anthes, Gary. "Happy Birthday Sputnik!" *Computerworld* 41, no. 44 (October 1, 2007): 44-50.
<http://search.proquest.com.ezproxy6.ndu.edu/docview/216118814?accountid=12686>
(accessed March 3, 2013).
- . "Timeline: Sputnik and Three Decades of DARPA Hegemony." *Computerworld (Online)*.
http://www.computerworld.com/s/article/9037638/Timeline_Sputnik_and_Three_Decades_of_DARPA_Hegemony (accessed February 7, 2013).
- Bajaj, Kamlesh. *The Cybersecurity Agenda: Mobilizing for International Action*. New York: East West Institute, 2010. <http://www.ewi.info/cybersecurity-agenda>
(accessed November 13, 2012).
- Beautement, Adam and David Pym. "Structured Systems Economics for Security Management." Harvard University, Ninth Workshop on the Economics of Information Security (WEIS), June 7-8, 2010.
- Bernstein, Adam. "Obituaries: Defense Expert William Kaufmann." *Washington Post*, December 17, 2008. <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/16/AR2008121602724.html> (accessed January 15, 2013).
- Brantley, Chris. "Congress Swings, Misses on Cybersecurity." IEEE.
<http://www.todaysengineer.org/2012/Sep/cybersecurity.asp> (accessed March 3, 2013).

- Bruner, J. S. and Leo Postman. "On the Perception of Incongruity: A Paradigm." *Journal of Personality* 18 (1949): 206-23.
- Carr, Jeffrey. *Inside Cyber Warfare*. Edited by Mike Loukides. 1st ed. Sebastopol, CA: O'Reilly Media Incorporated, 2009.
- Castro, Daniel. "U.S. Federal Cybersecurity Policy." in *Cybersecurity: Public Sector Threats and Responses*, 127-158. Edited by Kim Andreasson. 1st ed. Boca Raton, FL: CRC Press, 2012.
- Center for Strategic International Security. *Securing Cyberspace for the 44th Presidency*. Washington DC: CSIS, December 2008.
- Chien, Eric, Nicolas Falliere, and Liam Murchu. *W32. Stuxnet Dossier: Version 1.4*. Cupertino, CA: Symantec Corporation, 2011.
- Cunningham, Steve. "Cyber Security for Industrial Control Systems." *Power Engineering* 15, no. 11 (June 2011): 142-6.
<http://search.proquest.com.ezproxy6.ndu.edu/docview/910071964?accountid=12686>
(accessed February 23, 2013).
- Defense Advanced Research Projects Agency. "About DARPA." DARPA.
<http://www.darpa.mil/About.aspx> (accessed September 21, 2012).
- DiSabatino, Jennifer. "The Wild Wild West." *Computerworld* 35, no. 46 (November 12, 2001).
<http://search.proquest.com.ezproxy6.ndu.edu/docview/216089759?accountid=12686>
(accessed March 9, 2013).
- Duroy, Quentin. "The Place of Biotechnology in Modern Civilization: A Veblenian Analysis of Public Misgiving Toward Embryology in the United States." *Journal of Economic Issues* 45, no. 3 (September 2011): 559-572.
- Eastermann, Gregg. "State of High School Nation." ESPN.
<http://sports.espn.go.com/espn/page2/story?page=easterbrook/071113> (accessed February 5, 2012).
- Executive Office of the President. *Memo to the Heads of Executive Departments and Agencies, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, April 21, 2010*.
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf (accessed September 21, 2012).
- Executive Order no. 13010. "Critical Infrastructure Protection." *Federal Register* 61, no. 138, title 3 (July 15, 1996). <http://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf> (accessed October 27, 2012).

- Gardels, Nathan. "He Has Seen the Future." *Financial Times*, August 19, 2006. <http://www.ft.com/cms/s/0/af33b982-2dbd-11db-93ad-0000779e2340.html#axzz2Lm4HX9cn> (accessed October 5, 2012).
- Goodman, Seymour and Herbert Lin. *Toward a Safer and More Secure Cyberspace*. Washington DC: National Academy Press, 2007.
- Government Accounting Office. *Cybersecurity: Threats Impacting the Nation*, by Gregory Whilshuen. Washington DC: Government Printing Office, 2012.
- . *Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities*, by David D'Agostino and Gregory Wilshusen. Washington DC: Government Printing Office, 2011.
- . *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, by Gregory Whilshuen. Washington DC: Government Printing Office, 2011.
- . *Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, by David Powner and David Trimble. Washington DC: Government Printing Office, 2011.
- . *Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies*, by Gregory Wilshuen. Washington DC: Government Printing Office, 2008.
- Grobler, Marthie and Namosha Veerasamy. "Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure." Lecture, 6th International Conference on Information Warfare and Security, George Washington University, Washington DC, March 17-18, 2011. <http://researchspace.csir.co.za/dspace/handle/10204/5781>. (accessed October 31, 2012), 6.
- Harris, Shon. *CISSP: All in One Exam Guide*. Edited by Timothy Green, Joe Hoofnagle, and Clement Dupuis. 4th ed. New York: McGraw-Hill, 2008.
- Hoover, J. N. "CEOs Voice Support for Cyber Legislation, with Caveats." Information Week. [http://www.informationweek.com/government/policy/ceos-voice-support-for-cyber-legislation/240147638?queryText=cybersecurity act of 2012](http://www.informationweek.com/government/policy/ceos-voice-support-for-cyber-legislation/240147638?queryText=cybersecurity%20act%20of%202012) (accessed September 21, 2012).
- . "Cybersecurity Balancing Act." Information Week. <http://www.informationweek.com/security/government/cybersecurity-balancing-act/217100126> (accessed September 21, 2012).

- House of Representatives. *Recommendations of the House Republican Cybersecurity Task Force*. Washington DC: Government Printing Office, March 2012.
http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf.
- House Committee on Homeland Security. *Examining the Cyber Threat to Critical Infrastructure and the American Economy*. 112th Cong., 1st sess., March 16, 2011.
- . *Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*. 112th Cong., 1st sess., June 24, 2011.
- House Republican Cybersecurity Task Force. *Recommendations of the House Republican Cybersecurity Task Force*. Washington DC: Government Printing.
http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf (accessed February 4, 2013).
- Internet World Stat. "Internet World Stat: Usage and Population Statistics as of December 31, 2011." Miniwatts Marketing Group.
<http://www.internetworldstats.com/stats.htm> (accessed November 1, 2012).
- Jabbour, Kamal. *50 Cyber Questions Every Airman Can Answer*. Rome, NY: Air Force Research Laboratory, 2008.
- Keizer, Gregg. "Is Stuxnet the Best Malware Ever?" InfoWorld.
<http://www.infoworld.com/print/137598> (accessed September 14, 2012).
- Khanna, Ayesha and Parag Khanna. "Technology Will Take on a Life of Its Own." *Foreign Policy*, no. 188 (September/October, 2011).
- Kimmey, Phillip. "FISMA, Cyberscope, and Federal IT Security." Center for Strategic and International Studies. <http://csis.org/blog/fisma-cyberscope-and-federal-it-security> (accessed January 14, 2013).
- Kitten, Tracy. "Are Banks Winning the DDoS Battle?" Information Security Media Group Corporation. <http://www.bankinfosecurity.com/are-banks-winning-ddos-battle-a-5434/p-2> (accessed February 3, 2013).
- Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz. 1st ed. 24-42. Dulles, VA: Potomac Books, 2009.
- Kuhn, Thomas S. *The Structure of Scientific Revolutions*. 3rd ed. Chicago: The University of Chicago Press, 1962.

- Leithauser, Tom. "CRS Report Paints Complex Picture of Cybersecurity Policy Landscape." *Cybersecurity Policy Report* (December 19, 2011). <http://search.proquest.com.ezproxy6.ndu.edu/docview/920195648?accountid=12686> (accessed February 24, 2013).
- Lewis, James A. "Code Red." *Foreign Policy*. August 2012. http://www.foreignpolicy.com/articles/2012/08/01/code_red (accessed November 18, 2012).
- Libicki, Martin. *Cyberdeterrence and Cyberwar*. Arlington: RAND Corporation, 2009.
- Markoff, John. "Killing the Computer to Save It." *New York Times*, October 30, 2012. <http://www.nytimes.com/2012/10/30/science/rethinking-the-computer-at-80.html?pagewanted=all&r=0> (accessed November 18, 2012).
- . "Malware Aimed at Iran Hit Five Sites, Report Says." *New York Times*, February 13, 2011. <http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/851394210?accountid=12686> (accessed November 20, 2012).
- McCarthy, John, Chris Burrow, Maeve Dion, and Olivia Pacheco. "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz. 1st ed. 543-56. Dulles, VA: Potomac Books, 2009.
- Michael, Joseph Gross. "A Declaration of Cyberwar." *Vanity Fair* April 2011. <http://ezproxy6.ndu.edu/login?url=http://search.proquest.com/docview/919475999?accountid=12686> (accessed November 19, 2012).
- Nagesh, Gautham. "House Cybersecurity Bill Would Establish Federal Overseer." *The Hill*. <http://thehill.com/blogs/hillicon-valley/technology/199929-house-members-introduce-cybersecurity-bill> (accessed February 18, 2013).
- National Information Center. "The Top 50 Holding Companies." The Federal Reserve. <http://www.ffiec.gov/nicpubweb/nicweb/Top50Form.aspx> (accessed February 1, 2013).
- National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 1*. Washington DC: Government Printing Office, February 2010.
- . "Security Management and Assurance: FISMA Overview." U.S Department of Commerce. <http://csrc.nist.gov/groups/SMA/fisma/overview.html> (accessed January 18, 2012).

Newton, Harry. *Newton's Telecom Dictionary*. Edited by Steve Schoen. 25th ed. New York: Flatiron Publishing, 2009.

Office of Management and Budget. *FY 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. Washington DC: Government Printing Office, March 2012.

O'Harrow, Robert Jr. "Hacking Tool Kits, Available Free Online, Fuel Growing Cyberspace Arms Race." *Washington Post*, November 13, 2013.
http://www.washingtonpost.com/investigations/hacking-tool-kits-available-free-online-fuel-growing-cyberspace-arms-race/2012/11/12/1add77a4-21e6-11e2-ac85-e669876c6a24_story.html?wpisrc=emailtoafriend (accessed November 15, 2013).

Overby, Stephanie. "Tips From the Budget Masters." *CIO Magazine, Special Issue* Fall/Winter 2004.
<http://books.google.com/books?id=ZwoAAAAAMBAJ&pg=PA43&lpg=PA43&dq=cio+magazine+business+case&source=bl&ots=fE8nKIDBLD&sig=1OJ5XTv57wHl8wRDd3ppbLIVGBo&hl=en&sa=X&ei=g0wNUeKbO7Dx0wGBwYHoDQ&ved=0CDAQ6AEwAA#v=onepage&q=cio%20magazine%20business%20case&f=false> (accessed February 4, 2013).

Panetta, Leon. *Remarks by Secretary of Defense Leon Panetta to the Business Executives for National Security*. Washington DC: Office of the Secretary of Defense, 2012.

Pelley, Scott. "Panetta: Cyberware could Paralyze U.S." CBS Interactive, Inc.
http://www.cbsnews.com/8301-18563_162-57353420/panetta-cyber-warfare-could-paralyze-u.s/ (accessed October 28, 2012).

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting Americas Infrastructure*. Washington DC: Government Printing Office, October 1997.

Rice, David. *Geekonomics: The Real Cost of Insecure Software*. Boston, MA: Pearson Education, 2008. Kindle E-Book.

Rizzo, Jennifer. "Cybersecurity Deal Fails in Senate." Turner Broadcasting System, Inc.
<http://www.cnn.com/2012/08/02/politics/cybersecurity-act> (accessed January 20, 2013).

Schectman, Joel. "PwC: Companies Trim IT Security as Budgets Stagnate." Wall Street Journal. <http://blogs.wsj.com/cio/2012/09/20/pwc-companies-trim-it-security-as-budgets-stagnate/?KEYWORDS=cybersecurity> (accessed February 1, 2013).

Schiesel, Seth. "AT&T's Embrace of New Technology Signals Next Era." *New York Times*, March 8, 1999.

<http://search.proquest.com.ezproxy6.ndu.edu/docview/431147861?accountid=12686>
(accessed August 10, 2012).

Telecommunications Industry Association. "Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain." Telecommunications Industry Association. <http://tiaonline.org/policy/securing-network-cybersecurity-recommendations-critical-infrastructure-and-global-supply> (accessed January 18, 2012).

The MITRE Corporation. *Science of Cybersecurity*. Rosslyn, VA: The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2010. www.fas.org/irp/agency/dod/jason/cyber.pdf (accessed March 19, 2013).

The White House. "Introducing the New Cybersecurity Coordinator." The White House. <http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator> (accessed February 9, 2013).

Thompson, Karson K. "Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate." *Texas Law Review* 90, no. 2 (2011): 465-95. <http://search.proquest.com.ezproxy6.ndu.edu/docview/916011879?accountid=12686> (accessed October 4, 2012).

Toffler, Alvin and Heidi Toffler. *War and Anti-War*. New York, NY: Little, Brown & Company, 1993.

U. S. Congress. House Armed Services Committee. *Prepared Statement by Dr. Regina Dugan*. Washington DC: U. S. House of Representatives, 2011. http://armedservices.house.gov/index.cfm/files/serve?File_id=7ccf4551-0f9b-4212-9349-e846475c5655 (accessed January 22, 2013).

U.S Army Signal Center Fort Gordon, GA. "Information Assurance Fundamentals Training: Subheading Network/Hacker Threats." U.S Army. <https://ia.signal.army.mil/IAF/default.asp> (accessed December 18, 2012).

U.S. Department of Defense. *Department of Defense Dictionary of Military Terms and Associated Terms*. Washington DC: Government Printing Office, November 2012.

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

———. *Quadrennial Defense Review Report*. Washington DC: Government Printing Office, February 2010.

U.S. President. *International Strategy for Cyberspace*. Washington DC: Government Printing Office, May 2011.

- http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed August 15, 2012).
- . *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington DC: Government Printing Office, May 2009.
www.whitehouse.gov/assets/documents/cyberspace_policy_review_final.pdf (accessed August 11, 2012).
- . *The National Strategy to Secure Cyberspace*. Washington DC: Government Printing Office, February 2003. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed October 4, 2012).
- U.S. Presidential Decision Directive 63. "Protecting America's Critical Infrastructure." (May 22, 1998). <http://www.fas.org/irp/offdocs/pdd-63.htm> (accessed October 27, 2012).
- Van Atta, Richard. *50 Years of Innovation and Discovery*. Washington DC: DARPA.
www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2553 (accessed Jan 28, 2012).
- Verizon Business. *2012 Data Breach Investigations Report*. Ashburn: Verizon Business, 2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (accessed September 21, 2012).
- . "Verizon Enterprise Risk and Information Sharing (VERIS) Community." Verizon Business. <http://www.veriscommunity.net/doku.php?id=attributes> (accessed September 21, 2012).
- Waltrip, Mitch. *DARPA and the Internet Revolution*. Washington DC: DARPA.
www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2554 (accessed October 15, 2012).
- Wheeler, Deborah L. "Understanding Cyber Threats." in *Cybersecurity: Public Sector Threats and Responses*, 27-54. Edited by Kim Andreasson. 1st ed. Boca Raton, FL: CRC Press, 2012.
- White, Curt. *Data Communications and Computer Networks: A Business User's Approach*. 4th ed. Boston: Thomson Course Technology, 2007.
- White, Daniel. "The Federal Information Security Management Act of 2002: A Potemkin Village." *Fordham Law Review* 79, no. 1 (2010): 369-405.
<http://fordhamlawreview.org/articles/the-federal-information-security-management-act-of-2002-a-potemkin-village> (accessed October 4, 2012).

Zizek, Slavoj. "What Rumsfeld Doesn't Know that He Knows about Abu Ghraib." In These Times and the Institute for Public Affairs. <http://inthesetimes.com/article/747/> (accessed January 21, 2013).

VITA

LTC James Martin received a Regular Army commission in 1993 from McDaniel College with a Bachelor of Arts in Political Science. In 2008, he received a Masters of Arts in Information Technology from Webster University.

LTC Martin's served in a variety of Air Defense Artillery assignments in the 101st Airborne (Air Assault) Division and the 2nd Infantry Division to include Platoon Leader, Battery Executive Officer, Battery Maintenance Officer, Assistant Battalion Operations Officer, and Battery Commander.

In 2003, LTC Martin entered the United States Army Reserve (USAR), Active Guard Reserve (AGR) program as a Modeling and Simulations Officer (FA57), where he served as a Battle Command Observer/Controller and Assistant Operations Officer within the 1st Brigade, 87th Training Support Division.

In 2006, LTC Martin deployed as the 164th Corps Support Group, 63d Regional Readiness Command's (USAR) Liaison Officer (LNO) to the 13th Sustainment Command (Expeditionary) during Operation IRAQI FREEDOM.

In 2009, LTC Martin graduated from the United States Army Signal School's Information Managers Course (FA53) where he obtained the Certified Information Systems Security Professional (CISSP) and the Cisco Certified Network Associate (CCNA) professional certifications. LTC Martin subsequently served as the Network Operations Officer and Deputy G6 for the United States Army Civil Affairs and Psychological Operations Command Airborne (USACAPOC(A)) and as Branch Chief, Current Operations and later Branch Chief, Telecommunications within the G2/6 United States Army Reserve Command (USARC).

LTC Martin is currently attending the Joint Advanced Warfighting School (JAWS) at the Joint Forces Staff College - National Defense University.