CYBER INFRASTRUCTURE:
THE FORGOTTEN VULNERABILITY

A Monograph

by

MAJ Michael R. Wacker
United States Army

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

2014-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23-04-2014	SAMS Monograph	JUNE 2013 – MAY 2014

4. TITLE AND SUBTITLE

Cyber Infrastructure: The Forgotten Vulnerability

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Michael R. Wacker, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army School of Advanced Military Studies
ATTN: ATZL-SWD-GD
1 Reynolds Ave.
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT

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

Cyber infrastructure is a relatively new topic in the discussion of national security. The advent of cyber as a fifth warfighting domain has elevated the importance of cyber in national security priorities. The singular focus on virtual attacks has resulted in the neglected security of the actual physical infrastructure. As contemporary theorists struggle to understand the future of cyber and its place in national security, the physical aspect of cyber has been relegated to the background of the discussion. The current administration's reliance on the private-public partnership, where the private sector owns a vast majority of the infrastructure, has delayed efforts in a comprehensive security plan that encompasses both physical and virtual attacks. Although a coordinated attack has yet to occur, the possibility exists.

This monograph proposes that cyber infrastructure is vulnerable to attack. Specifically, a combined physical and virtual attack poses a significant threat to the U.S. cyber infrastructure. The lack of documented research about the possible effects of a coordinated, complex attack reveals a planning lapse that our enemies could exploit. This paper will utilize a scenario approach to determine possible outcomes of such an attack. The findings will show that the absence of a coherent and inclusive cyber infrastructure defensive strategy, which has left the U.S. vulnerable to physical attack, is the result of budgetary constraints, an overreliance on private-public partnership, and a lack of a codified single authority.

15. SUBJECT TERMS

Cyber, Infrastructure

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			MAJ Michael R. Wacker
U	U	U	UU	68	**19b. TELEPHONE NUMBER** *(include area code)*

MONOGRAPH APPROVAL PAGE

Name of Candidate: MAJ Michael R. Wacker

Monograph Title: Cyber Infrastructure: The Forgotten Vulnerability

Approved by:

_____, Monograph Director
Michael Mihalka, Ph.D.

_____, Seminar Leader
Jerry A. Turner, COL

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

Accepted this 22rd day of May 2014 by:

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

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

ABSTRACT

CYBER INFRASTRUCTURE: THE FORGOTTEN VULNERABILITY,
by MAJ Michael R. Wacker, 68 pages.

Cyber infrastructure is a relatively new topic in the discussion of national security. The advent of cyber as a fifth warfighting domain has elevated the importance of cyber in national security priorities. The singular focus on virtual attacks has resulted in the neglected security of the actual physical infrastructure. As contemporary theorists struggle to understand the future of cyber and its place in national security, the physical aspect of cyber has been relegated to the background of the discussion. The current administration's reliance on the private-public partnership, where the private sector owns a vast majority of the infrastructure, has delayed efforts in a comprehensive security plan that encompasses both physical and virtual attacks. Although a coordinated attack has yet to occur, the possibility exists.

This monograph proposes that cyber infrastructure is vulnerable to attack. Specifically, a combined physical and virtual attack poses a significant threat to the U.S. cyber infrastructure. The lack of documented research about the possible effects of a coordinated, complex attack reveals a planning lapse that our enemies could exploit. This paper will utilize a scenario approach to determine possible outcomes of such an attack. The findings will show that the absence of a coherent and inclusive cyber infrastructure defensive strategy, which has left the U.S. vulnerable to physical attack, is the result of budgetary constraints, an overreliance on private-public partnership, and a lack of a codified single authority.

ACKNOWLEDGMENTS

I would like to thank my wife and children for their love and support. They truly bear the brunt of the load and they allow me to continue to serve our country. I would like to thank the Iron Majors of Seminar 3. It was a great group and I enjoyed our time together immensely. Whenever I couldn't grasp something, my peers always came to my rescue and enlightened my understanding. Best of luck to each of you.

Finally, I would like to thank Dr. Michael Mihalka and Dr. Bruce Stanley. Dr. Mihalka's patience and understanding went far in assisting me through this monograph. His ability to explain complex concepts on a level I could understand was much appreciated. Dr. Stanley provided me with the advice I needed at a time when it was sorely needed. This monograph has a been a lesson in learning, and both gentlemen helped me immensely in understanding the process.

TABLE OF CONTENTS

ACRONYMS

ADM	Army Design Methodology
CI	Cyber Infrastructure
CIKR	Critical Infrastructure Key Resource
CNCI	Comprehensive National Cybersecurity Initiative
CS&C	Office of Cybersecurity and Communications
CSIS	Center of Strategic and International Studies
CSSP	Communications Sector-Specific Plan
DHS	Department of Homeland Security
DOD	Department of Defense
HSPD	Homeland Security Presidential Directive
ISP	Internet Service Provider
IT	Information Technology
NCCIC	National Cybersecurity and Communications Integration Center
NCS	National Communications System
NCSD	National Cyber Security Division
NIPP	National Infrastructure Plan
NSA	National Security Agency
NSPD	National Security Presidential Directive
PLA	People's Liberation Army
PMESII-PT	Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time
PPD	Presidential Decision Directive
QDR	Quadrennial Defense Review
RMA	Revolution of Military Affairs
SCADA	Supervisory Control and Data Acquisition

SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
UNCLOS	United Nations Convention on Law of the Sea

ILLUSTRATIONS

Page

INTRODUCTION

> Our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.[1]
>
> — President Barack Obama, 2009

> On a scale of one to 10, with 10 being strongly defended, our critical infrastructure's preparedness to withstand a destructive cyber attack is about a three based on my experience[2]
>
> — GEN Keith Alexander, commander of US CYBERCOM, 2013

> We will maintain resilient infrastructure to support mission assurance[3]
>
> — 2014 Quadrennial Defense Review

The globally interconnected information and communications infrastructure often known as "cyberspace" underpins every facet of American society and provides critical support for the national economy, civil infrastructure, security, and military power.[4] Cyberspace and its impact on national security have been a constant topic of discussion in the news media. The National Security Agency (NSA) spillage of classified material has highlighted the impact of cyberspace to the national defense as well as international relations.[5] Cybersecurity issues impact more than just national defense. The recent cyber theft of financial information from two of the Nation's largest

[1]Eric Talbot Jensen, "Cyber Deterence," *Emory International Law Review* 26 (2012): 777, http://www.law.emory.edu/fileadmin/journals/eilr/26/26.2/Jensen.pdf (accessed February 28, 2014).

[2]Deborah Charles, "NSA Chief Says U.S. Infrastructure Highly Vulnerable to Cyber Attack," *Reuters*, June 13, 2013, http://www.reuters.com/article/2013/06/12/us-usa-cybersecurity-idUSBRE95B10220130612 (accessed November 1, 2013).

[3]Department of Defense, *Quadrennial Defense Review 2014*, March 4, 2014, 13, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (accessed March 5, 2014).

[4]White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (White House, 2009), B–1, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed December 30, 2013).

[5]Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations," *The Guardian* June 9, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed January 18, 2014).

retailers affected millions with a loss of confidence in the financial institutions used to protect our sensitive information.[6] The inability of the current administration to get cybersecurity legislation passed in Congress highlights the conflicts in regulating the Internet and restricting access necessary for a virtual free market economy.[7] The tension arising from attempting to defend an open system designed for unimpeded access and private transactions is readily apparent in the difficulty of enacting security measures that might conflict with private industry interests.

Technology is altering the strategic implications of cyber capabilities, expanding and intensifying their influence.[8] The Internet is the main product of this radical transformation. The global digital infrastructure, "institutions, practices, and protocols that together organize and deliver the increasing power of digital technology to business and society," provide the means for this revolution.[9] These trends are "converging into a perfect storm that threatens traditional Internet values of openness, collaboration, innovation, limited governance and free exchange of ideas."[10] The ever-increasing reliance of private industry and the defense sector on this open system reveals the tension inherent between instant access and security.

Cyberspace has been considered a Revolution in Military Affairs (RMA), and comparisons with air and nuclear power are commonplace.[11] The Department of Defense (DoD)

---

[6]"Target, Neiman Marcus Executives Apologize for Data Breach," *Fox News*, last modified February 5, 2014, http://www.foxnews.com/politics/2014/02/05/target-neiman-marcus-executives-apologize-for-data-breach/ (accessed February 6, 2014).

[7]Brendan Sasso, "After Defeat of Senate Cybersecurity Bill, Obama Weighs Executive-Order Option," *The Hill*, last modified August 4, 2012, http://thehill.com/blogs/hillicon-valley/technology/242227-with-defeat-of-cybersecurity-bill-obama-weighs-executive-order-option (accessed February 6, 2014).

[8]James P. Farwell, "Industry's Vital Role in National Cyber Security," *Strategic Studies Quarterly* (Winter 2012): 32.

[9]Ibid., 12.

[10]P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 3.

[11]Colin S Gray, Army War College (U.S.), and Strategic Studies Institute, *Making Strategic Sense*

declared cyberspace a war fighting domain in 2005, making it the fifth alongside land, sea, air, and space.[12] The 2014 Quadrennial Defense Review indicated the importance of cyber at both the strategic and operational level, listing it as one of the key capabilities that protect our most vital national interests.[13] The fact that cyber is now on par with Special Operations Forces and Strategic Nuclear Forces speaks volumes in the leaps forward cyber has taken in national security strategy over the last decade. The discussion now has shifted toward how cyber can be part of larger operational planning and how its capabilities might be used to deter aggressive acts.[14]

The importance of cyberspace is undeniable as more of the world becomes connected. While much has been written about the strategic implications of cyber and the possibility of a virtual "Cyber 9-11", little is known about the vulnerability of the actual physical infrastructure of the Internet. The focus on the "virtual" cyberspace impacts to national security are well justified, but the actual physical cyber infrastructure risk is largely ignored. Recent media reports have addressed the lack of cyber infrastructure security and the implications to national security.[15] The Director of National Intelligence stated in testimony before the Congress, ''The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines,

---

of Cyber Power Why the Sky Is Not Falling (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 10, http://purl.fdlp.gov/GPO/gpo36745. Gray references Andrew Krepinevich's widely recognized 1994 RMA definition (accessed November 6, 2013).

[12]Department of Defense, *Department of Defense: Strategy for Operating in Cyberspace*, 2011, 5, http://www.defense.gov/news/d20110714cyber.pdf (accessed November 1, 2013).

[13]Department of Defense, *Quadrennial Defense Review 2014*, 32.

[14]Zachary Fryer-Biggs, "US Cyber Moves Beyond Protection," *Defense News*, last modified March 16, 2014, http://www.defensenews.com/article/20140316/DEFREG02/303170013/US-Cyber-Moves-Beyond-Protection (accessed March 20, 2014).

[15]Mark Clayton, "Cyberexperts: A 'Lost Decade' since 9/11 to Address Infrastructure Threats," *The Christian Science Monitor*, last modified January 17, 2014, http://www.csmonitor.com /USA/2014/0117/Cyberexperts-a-lost-decade-since-9-11-to-address-infrastructure-threats (accessed January 17, 2014).

financial networks, and other critical infrastructures.''[16] The Aurora test at the Idaho National Labs and the Stuxnet worm showed that cyber attacks can do physical damage.[17] The decade since 9-11 has seen little progress in either legislature protecting cyber infrastructure or federal standards enforcing infrastructure security.[18] Cyberspace and the Internet are largely thought of in terms of "online" or "virtual" characteristics, and not in terms of the actual physical hardware where data is secured and transmitted. The dismissal of a coherent physical defensive strategy could result in a vulnerability and leave our most important infrastructure at risk.

This paper will focus on the vulnerability of the actual physical infrastructure of the Internet. Specifically, the analysis will be on the effects of a combined physical and virtual attack. The absence of a coherent and inclusive cyber infrastructure defensive strategy, which has left the U.S. cyber infrastructure vulnerable to physical attack, is the result of budgetary constraints, an overreliance on private-public partnership, and a lack of a codified single authority. The underlying assumption that a strategy of deterrence will translate to physical cyber infrastructure is flawed.[19] Budgetary constraints that prioritize virtual attacks have marginalized physical defense considerations and have authorized private industry to define security requirements as it sees fit. The emphasis on private-public partnership is more a function of necessity than

---

[16]Authenticated U.S. Government Information,"Examining the Cyber Threat to Critical Infrastructure and the American Economy" (U.S. Government Printing Office, March 16, 2011), 1, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf (accessed March 9, 2014).

[17]Ibid., 42. The 2007 Aurora test at the Idaho National Laboratory (INL) was a demonstration that if a hacker could gain access to a controller, the attacker will cause physical damage.

[18]Clayton, "Cyberexperts: A 'Lost Decade' since 9/11 to Address Infrastructure Threats."

[19]White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," 2. Cybersecurity policy as used in this document includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulner- ability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities . . . as they relate to the security and stability of the global information and communications infrastructure.

preference.[20] Finally, the lack of a single authority that is charged with defending the collective whole undermines the concept of unity of command and allows for misinterpretations of administration policy.

The Department of Defense was the original proprietor of cyber infrastructure, however the vast majority is currently owned and operated by the private sector.[21] Military operations today are heavily dependent on globally (U.S. and foreign, government and civilian) shared infrastructures (physical and cyber).[22] This shift of ownership has resulted in a complex environment where federal policy must incorporate private considerations and compromise aspects of security. Many of DoD's critical functions and operations rely on commercial assets, including the cyber infrastructure such as data centers and underwater fiber optic cables, over which DoD has no direct authority to mitigate risk effectively.[23] Federal laws and regulations addressing critical infrastructure protection, disaster recovery, and the telecommunications infrastructure provide broad guidance that applies to the Internet, but it is not clear how useful these authorities would be in helping to recover from a major Internet disruption.[24] The significance of this study is to highlight the tensions existing in public-private partnership as well as the lack of a comprehensive authority and security policy.

---

[20]"Examining the Cyber Threat to Critical Infrastructure and the American Economy," 42. The rationale is that because private industry owns the majority of infrastructure then private industry should be responsible to secure it.

[21]Gregory Wilshusen, *GAO-08-212T, Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan* (Washington, D.C.: United States Government Accountability Office, 2007), 2, http://www.gao.gov/products/GAO-08-212T(accessed October 12, 2013). According to James A. Lewis of CSIS, private industry owns 85% of the critical infrastructure.

[22]Department of the Army, *AR 525-26 Military Operations Infrastructure Risk Management* (Department of the Army, June 22, 2004), 6, http://armypubs.army.mil/epubs/525_Series _Collection_1.html (accessed October 12, 2013).

[23]Department of Defense, "Department of Defense: Strategy for Operating in Cyberspace," 7.

[24]Wilshusen, *GAO-08-212T, Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, i.

The Department of Homeland Security is now charged with protecting the cyber infrastructure, which has proved challenging given the lack of federal legislation that governs both the federal and private sectors. The fact that a majority of the network is owned and operated by private entities such as Google and L-3 Communications only adds to the complex environment.[25] Sean P. Gorman's infamous 2004 dissertation that mapped the entire cyber infrastructure from open sources is a testament to the ability nefarious actors have in identifying soft targets in the network.[26]

The United States has come to depend on cyberspace to communicate in new ways, to make and store wealth, to deliver essential services, and to perform national security functions.[27] The Department of Defense (DoD) has publicly stated that they support the Department of Homeland Security (DHS) and the government cybersecurity team in the effort of securing critical infrastructure cybersecurity.[28] DoD is supporting this priority by investing in a new "Cyber Mission Force" as well as state-of-the-art tools and infrastructure necessary to support not only the Department networks but Combatant Commanders worldwide.[29] These initiatives underscore the shift in defense priorities from sustained ground combat to future hybrid threats where technology and cyberspace play a more prominent role. The Chief of Staff of the Army, GEN Raymond Odierno, included cyberspace as one of his strategic priorities for U.S. Army.[30] Cyber is now seen as an enabler to land power technologies to counter emerging threats and to

---

[25]Andrew Blum, *Tubes: A Journey to the Center of the Internet*, 1st ed. (New York: Ecco, 2012), 45.

[26]Jocelyn Rappaport, *On the Map: As Controversy Swirled around His Dissertation, Sean Gorman Realized His Future and Founded a Company*, 2004, http://spirit.gmu.edu/archives/winter08/on_the_map.html (accessed November 1, 2013).

[27]Department of Defense, *Quadrennial Defense Review 2014*, 7.

[28]Ibid., 17.

[29]Ibid., 31.

[30]GEN Raymond Odierno, "CSA Strategic Priorities" (Department of the Army, October 13, 2013), 8, http://usarmy.vo.llnwd.net/e2/c/downloads/316390.pdf (accessed March 6, 2014).

ensure that Army formations retain a decisive materiel edge and tactical overmatch across the range of military operations.[31]

The organization of the study is as follows: introduction, literature review, methodology, scenarios, findings and analysis, and conclusion. Following the introduction this monograph has seven sections. The introduction includes the background of the study, both the current cyber environment as a whole as well as cyber infrastructure, and the physical vulnerability inherent in both. The statement of the problem, the purpose of the study, significance of the study, definition of the terms, theoretical framework, research questions, limitations, and the assumptions of the study will comprise the rest of the introduction. The second section is a literature review that discusses relevant defensive theories, key conceptual terms, and current empirical data of leading cyber commentators. The methodology will focus on scenarios using structured focused comparisons. Finally, the findings and conclusion will present recommendations for the way ahead.

LITERATURE REVIEW

Cyber is a relatively new phenomenon, and as such there is not an acknowledged authority on the subject. Cyber's "Clausewitz" has yet to appear, and there are those who think the subject doesn't warrant a grand strategist in the same vein as a Douhet or Mahan.[32] Andrew Krepinevich's definition of a Revolution of Military Affairs (RMA) describes a military revolution as the application of a new technology that alters the character and conduct of war, usually increasing the lethality or effectiveness of the armed forces.[33] Using Krepinevich's

[31]Odierno, "CSA Strategic Priorities."

[32]Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 23, http://www.au.af.mil/au/ssq (accessed March 31, 2014).

[33]Gray, Army War College (U.S.), and Strategic Studies Institute, *Making Strategic Sense of Cyber Power Why the Sky Is Not Falling*, 25.

definition, cyber has yet to alter the character of war nor increase the effectiveness of armies, at least from an offensive point of view.

The argument to consider cyber revolutionary is directly correlated to digital networking. Cyber warfare, in terms of military effectiveness, requires the networked foe to have no retrogradeable structure to return to for operations.[34] Most authorities associate the mid-1990's as the genesis of digital networking, and the advancement in terms of reliance on these new systems is still in its infancy for even developed nations.[35] The strategic utility of cyber is negated by the fact that much like the element of surprise, it can only be used once since most states will simply isolate their systems from virtual attack.[36]

Cyber warfare study has sparked various schools of thought. Some have likened the impact of cyber to nuclear power. The idea is that cyber will impact conventional warfare in similar ways that the introduction of nuclear power did and will lead to a "cyber arms race". Technology and escalating measures by competing actors will lead to the adoption of a variant of mutual assured destruction, or deterrence strategy. The belief that virtual cyber attacks can cause physical destruction is at the root of this theory. There is some evidence of this theory, as witnessed by the Aurora test discussed earlier. Still others believe that cyber is only an enabler to traditional warfare, similarly to the other geographical domains of land, sea, or air.[37] Cyber is considered a tool to assist commanders in seizing the initiative and pertinent only in the element of surprise by disabling command and control systems and power structures. This hypothesis assigns cyber's main purpose as enabling physical warfare, similar to space and electromagnetic

[34]Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," 29.

[35]Ibid., 32.

[36]Ibid., 29.

[37]Gray, Army War College (U.S.), and Strategic Studies Institute, *Making Strategic Sense of Cyber Power Why the Sky Is Not Falling*, 9, 44.

spectrum.[38]Those who believe that the impact of cyber is overstated point to the lack of lethality and system resiliency as evidence of their argument.[39]

Cyber infrastructure security is usually mentioned along with the rest of the Critical Infrastructure Key Resource (CIKR) sectors in the discussion of physical vulnerability. The main arguments involving cyber infrastructure run similar to the discussion on cyber as a warfighting domain in general. There are those who feel the physical security of CI is adequate and that the reliance of the last three Presidential administrations on the private-public partnership is an agreeable and cost-effective way to mitigate what operational risk might exist in the CI sector. The adoption of deterrence as a strategic defensive theory from existing nuclear doctrine supports this theory, with the basis that other nation-states would not risk attacking U.S. infrastructure for fear of retaliation on theirs. Others point to the same private-public partnership and inadequacy of existing legislation as the root cause of CI vulnerability.[40]

The focus of most theorists is on the hypothetical virtual attack that could disable many of the systems Americans rely on everyday like banking institutions or energy providers. There is evidence to support this perspective, such as reports that the Chinese People's Liberation Army (PLA) is actively collecting intelligence on critical infrastructure such as power systems and telecommunications systems as part of computer network operations during potential future conflicts.[41] This argument assumes that our enemies would telegraph their intentions by actively probing their targets and risk a response in kind, basically ignoring physical vulnerabilities in an

[38]Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," 28.

[39]Colin S Gray, *Another Bloody Century: Future Warfare* (London: Phoenix, 2006), 322.

[40]James Martin, Jr., "Paradigm Change: Cybersecurity of Critical Infrastructure" (Joint Advanced Warfighting School, Norfolk, VA: Joint Forces Staff College, 2013). LTC Martin argues that legislation based on "Self-Regulation" and "Incremental Progress" theories are flawed and don't incorporate the current cyber threat against critical infrastructure.

[41]Bill Gertz, "Chinese Military Is Targeting Critical U.S. Infrastructure for Cyber Attacks, Report Says," *Flash//CRITIC Cyber Threat News*, last modified November 9, 2013, http://flashcritic.com/chinese-military-is-targeting-critical-u-s-infrastructure-for-cyber-attacks-report-says/ (accessed March 24, 2014).

effort for the quick victory of virtual attack. Another assumption is that not only could a hacker infiltrate our systems, they could do so undetected and thus prevent security adjustments as well as discovery of their methods.

The argument that cyber infrastructure is vulnerable to physical attack is in the minority and mainly regulated to those with technical knowledge of the systems in question. The physical layer of cyber infrastructure reveals that while a majority of our data centers are dispersed throughout the nation, many of the vital submarine fiber-optic cables that provide the backbone of the Internet terminate are in finite areas, primarily in the Northeast in a thirty mile region close to New York City. The reasons for this layout are primarily functional, as the commercial data centers are located in close proximity to their clients in the major cities. What is undetermined is the prioritization of the data centers, meaning what data centers route the most sensitive data that would be of value to our enemies. The lack of a coherent defensive strategy in the layout of physical infrastructure is a departure from our nuclear assets, where much of the infrastructure is located with security measures taken in consideration.[42]

Research has shown that physical damage to critical communication networks can lead to network failures and major disruptions to functions due to the interdependency of different critical infrastructures.[43] Others have identified weaknesses in commercial and federal infrastructure, information readily available from public records. Economic constraints have led to limitations in new network infrastructure, resulting in single points of failure and potential vulnerabilities. Disruptions to the Internet could be caused by a cyber incident (such as a software

[42]"History of U.S. Missile Defense Efforts 1945-Present," *Missile Defense Agency-U.S. DoD*, last modified March 25, 2014, http://www.mda.mil/news/history_resources.html (accessed March 25, 2014). Nuclear missile sites were also selected based on operations, support and sustainability, including easy access to potential operating areas and available support infrastructure.

[43]Michael Matis, 2012. The Protection of Undersea Cables: A Global Security Threat (Carlisle Barracks, PA: U.S. Army War College, 2012), 3.

malfunction or a malicious virus), a physical incident (such as a natural disaster or an attack that affects key facilities), or a combination of both cyber and physical incidents.[44] Recent cyber and physical incidents have caused localized or regional disruptions but have not caused a catastrophic Internet failure.[45] The Center of Strategic and International Studies (CSIS) published an exhaustive list of 163 cyber incidents since 2006 and physical attacks were not mentioned.[46]

There have been documented conspiracies to use kinetic means to destroy the Internet, such as the 2007 Al-Qaeda plot to bring down the United Kingdom Internet.[47] This conceived attack was the focus of intense enemy reconnaissance on the headquarters of Telehouse Europe, the main internet facility that houses the channel through which almost every bit of information on the internet passes in or out of Britain.[48] James Geary argues that an attack on the physical infrastructure could be more devastating due to the fact that over 90% of all internet traffic goes through terrestrial pathways.[49] Don Jackson, the director of threat intelligence-security firm SecureWorks, supports Geary by arguing that the competent systems in place to counter online attacks make physical attacks a more likely scenario due to existing vulnerabilities.[50] Andrew Blum's well-received book, Tubes, sought to identify the internet infrastructure by mapping the data centers and undersea fiber-optic cables. Blum argues that the internet's well-designed

---

[44]Wilshusen, *GAO-08-212T Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, i.

[45]Ibid.

[46]James Lewis, "Significant Cyber Incidents Since 2006" (Center for Strategic and International Studies, October 10, 2013), http://csis.org/files/publication/131010_Significant_Cyber_Incidents_Since_2006%20(3).pdf (accessed October 10, 2013).

[47]David Leppard, "Al-Queda Plot to Bring Down UK Internet," *Martinfrost*, March 11, 2007, http://www.martinfrost.ws/htmlfiles/mar2007/aqweb_plot.html (accessed November 1, 2013).

[48]Ibid.

[49]James Geary, "Who Protects the Internet?", March 13, 2009, 52, http://www.popsci.com/scitech/article/2009-03/who-protects-intrnet?nopaging=1 (accessed November 1, 2013.

[50]Ibid.

network of links have redundancies that eliminate potential and vulnerable single point of failures.[51]

The argument why physical infrastructure is more vulnerable than physical attacks usually reference the vulnerability of industrial control systems due to an immaturity of adopted control measures. The term ‘‘control system’’ encompasses several types of systems, including Supervisory Control and Data Acquisition (SCADA), process control, and other automated systems that are found in the industrial sectors and critical infra- structure.[52] Control systems security is particularly important because of the inherent interconnectedness of the CIKR sectors and their dependence on one another. SCADA against the physical infrastructure.[53]

Another reason physical attacks are marginalized in vulnerability assessments is due to the perceived resiliency of the infrastructure. Frank Washburn states that cable damage is primarily done from dragging ship anchors, fishing operations, and seismic activity.[54] Washburn argues that private companies like Verizon take security very seriously, and even if a breach were successful, the infrastructure has the capacity, diversity, intelligence, and ability to reroute over redundant links.[55] This confidence in the ability for the network to be self-healing is contradicted by others who state that while the infrastructure can be repaired, significant delays in manufacturing will enhance the impact of the breach.

While physical and virtual attacks have been discussed separately, there is little of note in regards to a possible coordinated attack combining the two. There has been documented concern

---

[51]Blum, *Tubes*, 116.

[52]“Examining the Cyber Threat to Critical Infrastructure and the American Economy,” 10.

[53]Ibid.,10.

[54]Frank Washburn, “Will Internet Sabotage Hit Home?,” *PC Magazine*, June 1, 2008, http://www.pcmag.com/article2/0,2817,2316780,00.asp (accessed November 1, 2013).

[55]Ibid.

for some of the CIKR sectors such as the electrical grid, but there is little on a combined physical-virtual attack on the actual cyber infrastructure.[56] The majority of the literature discusses each type of attack separately, dismissing a coordinated attack using the same assumptions mentioned earlier. Scenario analysis at the end of this monograph will address the potential effects of a combined physical and virtual attack.

Theoretical

The current cyber infrastructure utilizes a large amount of the pre-existing telecommunications infrastructure. The "walled garden" business model of legacy incumbent cable and telephone companies has culminated in its mission to provide Internet access to the masses in a timely and cost-effective manner.[57] Commercial Internet Service Providers (ISP)s have exhausted the existing infrastructure and now look to fulfill the "last mile" of connectivity.[58] Obviously chosen for economic and practical reasons, the reliance on pre-existing infrastructure poses a security risk for federal agencies charged with protecting these systems. In the same way that Sean Gorman was able to map the components noted earlier, our enemies would have the impetus for doing the same and determining the most critical nodes in the network. The way-ahead must incorporate security considerations not only to protect our key infrastructure but to deter our enemies from exploiting a known weakness.

---

[56] Stew Magnuson, "Feds Fear Coordinated Physical, Cyber-Attacks on Electrical Grids," *National Defense*, September 2012, http://www.nationaldefensemagazine.org/archive/2012/september/Pages/FedsFearCoordinatedPhysical,Cyber-AttacksonElectricalGrids.aspx (accessed April 24, 2014).

[57] Fred Pilot, "http://eldotelecom.blogspot.com/2014/03/us-at-Inflection-Point-on-Premises.html," *Eldo Telecom*, March 22, 2014, http://eldotelecom.blogspot.com/2014/03/us-at-inflection-point-on-premises.html (accessed March 25, 2014).

[58] Jim Krencik, "Telecom Reps Offer Testimony at Rural Broadband Hearing," *The Daily News*, March 21, 2014, http://thedailynewsonline.com/news/article_4c6ab52e-b0ac-11e3-baa4-001a4bcf887a.html (accessed March 25, 2014).

If cyber infrastructure is be a considered a strategic asset as the current Presidential Administration has stated, then some thought should go into how the components of the infrastructure are arrayed and defended. As Clausewitz stated in *On War*, the side that sees a significant advantage in a surprise attack will for that reason take the offensive.[59] Jomini subscribes to a more defense-in-depth concept by "multiplying obstacles and difficulties" and weakening the enemy by taking this exhaustive approach.[60] Jomini's principle that it is wiser to build fewer forts and have them properly located supports this line of thought.[61] His "lines of defense" describe a permanent line of defense, incorporated into the defense system of the state.[62] Both theorists subscribed to the defensive-offensive mindset, where strategic defense was conducted in only the amount of time necessary to transition to the offensive.[63] Clausewitz expands on the time element by stating that the greatest advantage in the defense is the time gained by the defender.[64]

These concepts have direct applicability to the defense of cyber infrastructure, both physical and virtual. A look at the layout of data centers and submarine cables show the majority arrayed in close proximity to other critical infrastructure for obvious reasons. This an approach taken in the name of efficiency. Cyber infrastructure should follow some form of defensive theory that protects our assets and provides a deterrent to our adversaries from attempting to sabotaging our systems.

---

[59]Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1976), 371.

[60]*Roots of Strategy* (Mechanicsburgh, PA: Stackpole Books, 1987), 463.

[61]*Roots of Strategy* (Mechanicsburgh, PA: Stackpole Books, 1987), 483.

[62]*Roots of Strategy*, 470.

[63]Ibid., 463.

[64]Ibid, 370.

Strategy

There has been much debate over what cyberspace means to national security strategy. The Department of Defense's mission does not include the defense of the civilian physical infrastructure that enables the vital networks that support not only our military networks but commercial ones as well. This security requirement is a daunting one: DoD operates over 15,000 networks and seven million computing devices. In addition there are over five-hundred thousand miles of cable and downs of internet exchange points, each of which must be defended in order to prevent the loss of sensitive data as well as commercial traffic. The vulnerability of the infrastructure could impact national security and compromise the ability of the DoD to coordinate rapid responses to global threats.

President Obama has repeatedly emphasized the importance of cybersecurity during his administration.[65] His declaration that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" has led to the creation of the first-ever Cybersecurity Office within the National Security Staff.[66] The President's cybersecurity strategy is twofold: (1) improve our resilience to cyber incidents and (2) reduce the cyber threat.[67] Explicit in his guidance relating to cyber infrastructure is the hardening of networks to defend against physical and virtual attack. This will be accomplished by partnering with international allies and private businesses, implementing more strident cyber laws, and by adopting a policy of deterrence against our adversaries.[68]

---

[65]James Langevin et al., "Securing Cyberspace for the 44th Presidency" (Center for Strategic and International Studies, n.d.), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed January 1, 2014).

[66]"Cyber Security," *The White House*, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity (accessed January 18, 2014).

[67]Ibid.

[68]"Cyber Security," The White House, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity (accessed January 18, 2014).

Patrick Morgan defines deterrence as “the threat to use force in response as a way of preventing the first use of force by someone else.”[69] Morgan describes deterrence as two types: general and immediate. The term “general deterrence” is more applicable to nation states in cyber warfare. General deterrence refers to those entities that maintain armed forces to regulate their relationship with adversaries even though neither is anywhere near mounting an attack.[70] Immediate deterrence describes the relationship between states and non-state actors in cyber warfare, where the threat is imminent. Immediate deterrence is a relationship "where at least one side is seriously considering an attack while the other is mounting a threat of retaliation in order to prevent it."[71] This describes President Obama’s cybersecurity strategy above that emphasizes reducing the threat and conveying the implicit retaliation that will occur to those who attempt to harm our networks.

The success or failure of general and immediate deterrence is hard to determine. Huth and Russett’s expected-utility model of extended deterrence argues that successful deterrence is a factor of the relationships between states and not just a military balance of power.[72] Extended deterrence, the deterrence of an attack on a third party or political ally, is challenging in this regard as projecting our resolve in cyber warfare could mean an escalation of force that the U.S. is unprepared to commit to.[73] The recent conflict in Ukraine as well as the 2008 Estonia attack highlight the challenge the U.S. has in deterring attacks against its allies. The issue of deterring cyber attacks is a problem of capability, commitment, and communication. As Huth and Russett

---

[69]Ibid.

[70]Paul Huth and Bruce Russett, “What Makes Deterrence Work? Cases from 1900 to 1980,” *World Politics* 36, no. 4 (July 1984): 496, http://www.jstor.org/stable/2010184 (accessed April 21, 2014).

[71]Ibid., 496.

[72]Ibid.

[73]Paul Huth and Bruce Russett, “What Makes Deterrence Work? Cases from 1900 to 1980,” *World Politics* 36, no. 4 (July 1984): 496, http://www.jstor.org/stable/2010184 (accessed April 21, 2014)..

point out, "the requirements for implementing deterrence are much less a matter of acquiring, proving possession of, or using raw military capabilities than a matter of demonstrating concern, motivation and commitment."[74] Capability refers to the balance of military power that exists on the whole and at the local level. One of the reasons cyber warfare is the weapon of choice for non-state actors is because it levels the playing field in a specific domain, similar to the local level in counterinsurgency. Non-state actors leverage cyberspace as an operational safe haven and as a means to attack, subscribing to many of the tenets of irregular warfare.[75] Attribution is difficult if not impossible in the virtual realm of cyberspace, and retribution could be used by adversaries to rally opposition, and excessive use of force can outweigh any gains derived from the military application of cyber.[76] Commitment refers to the resolve necessary to prosecute attacks against state and non-state actors in the cyber realm. The current cyber strategy does not address offensive capability, only the impetus to reduce the threat and harden our defenses. The lack of explicit retaliation could serve to empower our adversaries, especially those unaffiliated with a state with political ties with the U.S. that could offset the threat. Communication is how this resolve is conveyed to the adversary. The past administrations have gone to great lengths to convey that the U.S. will not standby as terrorists attack our country in pursuit of their ideological and political goals.[77] This foreign policy has worked well for homeland defense, but application to cyber remains untested.

---

[74]Paul Huth and Bruce Russett, "What Makes Deterrence Work? Cases from 1900 to 1980," World Politics 36, no. 4 (July 1984): 502, http://www.jstor.org/stable/2010184 (accessed April 21, 2014).

[75]Department of Defense, "Irregular Warfare: Countering Irregular Threats" (Department of Defense, May 17, 2010), 14, http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf (accessed April 21, 2014).

[76]Department of Defense, "Irregular Warfare: Countering Irregular Threats" (Department of Defense, May 17, 2010), 14, http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf (accessed April 21, 2014).

[77]President George W. Bush, "The National Security Strategy of the United States of America" (The White House, Septembe02/ (accessed April 21, 2014).

The reliance on deterrence as a viable strategic option is not a new concept in national defense. Deterrence was the strategy of choice during the Cold War with the Soviet Union before falling out of favor after the implementation of the Bush doctrine of pre-emption.[78] The ability to strike an adversary in response to an attack that is imminent or has already commenced was the backbone of nuclear deterrence.[79] Often referred to as Mutually Assured Destruction, the threat of retaliation would dissuade attackers. Martin Libicki argues that concept of cyber deterrence contrasts starkly with the clarities of nuclear deterrence.[80] The certainties of attrition made repudiation impossible in nuclear war, whereas cyber attacks require little investment and only the will to carry it out. During the Cold War, nuclear deterrence strategy only had to consider two actors with global political interests at stake, whereas cyber deterrence must incorporate a plethora of non-state actors with limited aims and marginal risk. Nuclear security was the domain of the state, whereas in cyber private industry is responsible to defend itself.[81]

The applicability of deterrence as a strategy does not hold relevance with cyber infrastructure. The case for cyber deterrence generally rests on the assumption that cyber attacks are cheap and that cyber defense is expensive.[82] An attack on cyber infrastructure gives the source the same anonymity that a virtual attack does, making a physical attack less in operational as well as strategic risk. Although a physical attack would also likely meet the United Nations self-defense requirement of "use-of-force" and "armed attack", the thresholds necessary for a

[78]President George W. Bush, "The National Security Strategy of the United States of America" (The White House, September 17, 2002), 2, http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/ (accessed April 21, 2014).

[79]Jensen, "Cyber Deterence," 793.

[80]Martin C. Libicki and Project Air Force (U.S.), *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), xvi.

[81]Ibid, xvi.

[82] Martin C. Libicki and Project Air Force (U.S.), *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), xvi.

response in-kind, the anonymity of the attacker negates the response. The crux pertaining to cyber infrastructure deterrence is what the definition of "response in-kind" is and what the retaliatory attack would look like, given that most perpetrators are non-state actors such as terrorists. International law espouses "proportional countermeasures", with a state-centric three-part test based on an escalation of force.[83]

CONCEPTUAL TERMS

Cyberspace

FM 3-38 and Joint Publication 1-02 define cyberspace as a global domain within the information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[84] This definition is a derivative from National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), which defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.[85] This definition focuses on the human element as well as the network systems. Contemporary theorists define cyberspace in similar terms, but minimize not only the human element but the physical infrastructure as well. For example, Kamlesh Bajaj defines cyberspace as IT networks, computer resources, and all the fixed and

[83]Jensen, "Cyber Deterence," 798.

[84]Headquarters, Department of the Army, *FM 3-38 Cyber Electromagnetic Activities* (Headquarters, Department of the Army, February 2014), 1–4, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf (accessed February 28, 2014).

[85]White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," 1.

mobile devices connected to the global internet.[86] The 2003 National Strategy to Secure Cyberspace defined cyberspace as the "nervous system-the control system of the country….composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.[87] This definition more accurately focuses on the infrastructure that actually comprise the Internet.

Cyberspace is a system of systems with many small and diverse systems comprising the structure as a whole.[88] The system is dynamic and constantly changing due to advances made by private industry. The interrelationship with private industry is evident with physical infrastructure. The federal government relies on private industry to not only create and maintain components of infrastructure, but also to provide for its security. This is reflected in the tensions between government agencies, the military, and private industry on overlapping authority of the various domains (.com, .mil, .gov, etc).

Private-Public Partnership

U.S. defensive policy is predicated on the private-public partnership, a co-operative relationship between the U.S. Government and the private sector that owns the majority of the cyber infrastructure.[89] The methodology of private-public partnership is to improve CIKR cyber network and system security through information sharing and improved situational awareness that

[86]Kamlesh Bajaj, "The Cybersecurity Agenda: Mobilizing for International Action" (The EastWest Institute, 2010), 1, http://www.ewi.info/sites/default/files/ideas-files/Bajaj_Web.pdf (accessed January 1, 2014).

[87]*Cyberpower and National Security*, 1st ed. (Washington, DC: National Defense University Press : Potomac Books, 2009), 25.

[88]Headquarters, Department of the Army, *FM 3-38 Cyber Electromagnetic Activities*, 1–5.

[89]"Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnership" (Department of Homeland Security, 2009), 3, http://publicintelligence.net/project-12-and-the-public-private-cybersecurity-complex/ (accessed March 25, 2014).

can inform the other's risk-based decisions.[90] While existing public- private partnerships have facilitated information sharing and policy coordination to address these obstacles, more can be done to improve the security and resilience of CIKR networks.[91]

Current literature has criticized the public-private partnership. The cyber infrastructures of the United States and Europe offer inviting targets for attack, whether for profit, malice, or state objectives.[92] The boundaries between the actual cyber infrastructure and external systems using the infrastructure have become so intertwined that it may be impossible to separate them.[93] Sovereignty issues at the local level complicate what is already becoming a blurred line between the physical and virtual domains.[94] Private enterprise prerogative to retain regulatory freedom of action compromises the ability of federal authorities to impose tighter security measures [source].

The concerns about the security of cyber infrastructure have been well-documented, even before the attacks on 9-11. The attempt for a collective security plan has resulted in a fragmented approach with a lack of overall accountability at any one level.[95] Cybersecurity refers to three items: measures to protect information technology; the information it contains, processes, and transmits, and associated physical and virtual elements; the degree of protection resulting from application of those measures; and the associated field of professional endeavor.[96] Eric A. Fischer

---

[90]Anonymous, "Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnership" (Department of Homeland Security, 2009), 3, http://publicintelligence.net/project-12-and-the-public-private-cybersecurity-complex/ (accessed March 25, 2014).

[91]Ibid, 3.

[92]U.S. Army War College, *Cyber Infrastructure Protection* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011), 129.

[93]Army War College (U.S.), Cyber Infrastructure Protection (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011), 129.

[94]U.S. Army War College, *Cyber Infrastructure Protection*, 130.

[95]United States, *Cybersecurity and Homeland Security* (New York: Nova Science Publishers, Inc, 2005), vii.

[96]Ibid.

describes options addressing the security problem. They include standards and certification, promulgating best practices and guidelines, using benchmarks and checklists, use of auditing, improving training and education, building security into enterprise architecture, using risk management, and using metrics. Fischer argues that none of these will be adopted without sufficient economic incentives and that cyberspace has too many properties of a commons for market forces alone to provide those incentives.[97]

A national cybersecurity framework can be thought of as the essential set of public- and private-sector efforts required to ensure an acceptable level of cybersecurity for the nation.[98] Erik Fischer evaluates cybersecurity framework by asking three questions. The first question pertains to major cybersecurity weaknesses both current and projected. The next question addresses available means of addressing these weaknesses. The last question pertains to the role the government and private sector should play in the use of those means of leverage to address current and potential future weaknesses.[99]

Identification of weaknesses requires analysis of the components of cybersecurity. Cyberspace is centered on the Internet and the computers connected to it, but it also includes electronic systems or devices and the peripheral devices that either directly or indirectly connect as well. Cyberspace infrastructure is broken down into four segments: Internet hardware, telecommunications infrastructure, embedded computing devices such as control systems, and dedicated computing devices such as desktop computers.[100] Each of these components provide

[97]United States, *Cybersecurity and Homeland Security*, 2.

[98]Ibid.

[99]Ibid., 4.

[100]United States, *Cybersecurity and Homeland Security* (New York: Nova Science Publishers, Inc, 2005), 10.

access points there are susceptible to compromise and therefore pose a security risk to the overall architecture.

The connection between cyber infrastructure and the critical infrastructure of other entities such as banking and finance or energy provides context into the synergistic impacts a simultaneous attack could have. Information technology (IT) is essential to virtually all of the nation's critical infrastructures, which makes any of them vulnerable to a terrorist attack on the computer or telecommunications networks of those infrastructures.[101] Internet infrastructure plays a critical role in managing and operating nuclear-power plants, dams, the electric-power grid, the air-traffic-control system, and financial institutions.[102] IT is the technological underpinning of the nation's communications systems, from the local loop of "plain old telephone service" to the high-speed backbone connections that support data traffic. These realities make the computer and communications systems of the nation a critical infrastructure in and of themselves, as well as major components of other kinds of critical infrastructure, such as energy or transportation systems. In addition, while IT per se refers to computing and communications technologies, the hardware and software (i.e., the technological artifacts of computers, routers, operating systems, browsers, fiber-optic lines, and so on) are part of a larger construct that involves people and organizations.

Authority

Cyber infrastructure authority derives many of its characteristics from telecommunications security initiatives. The shift from telecommunications to cyber occurred during President Clinton's administration. On July 15, 1996, Presidential Executive Order 13010

[101]National Research Council (U.S.) and National Academies Press (U.S.), *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*, ed. John L. Hennessy, David A. Patterson, and Herbert Lin (Washington, DC: National Academies Press, 2003), 11.

[102]Ibid,11.

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.[103] Presidential Executive Order 13010 formally acknowledged the reality that the preponderance of national critical infrastructure ownership resides within the commercial sector. President Clinton was the first President to address cyber infrastructure when he commissioned the Critical Infrastructure Protection Commission in 1996. Based upon the findings in that study, President Clinton signed Presidential Decision Directive 63 (PDD-63) Critical Infrastructure Protection, in May 1998. PPD-63 established a structure under White House leadership to coordinate the activities of designated lead departments and agencies, in partnership with their counterparts from the private sector, to "eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[104] PDD 63 affirmed that, while the Department of Commerce is the lead agency for information and communications, DoD would retain its Executive Agent responsibilities for the NCS. This policy was updated in 2003 with The National Strategy to Secure Cyberspace. It was further augmented later that year in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003) which assigned the Secretary of Homeland Security the responsibility for coordinating the nation's overall critical infrastructure protection efforts, including for cyber infrastructure, across all Information Technology and Communications sectors working in cooperation with designated sector-specific agencies within the Executive Branch.

The Homeland Security Act of 2002 established the Department of Homeland Security (DHS) under Title 5, United States Code. Under the technology infrastructure umbrella, DHS

[103]Martin, Jr., "Paradigm Change: Cybersecurity of Critical Infrastructure," 40.

[104]"Presidential Decision Directives - PDD 63," *Presidential Decision Directives - PDD*, last modified May 22, 1998, https://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed March 1, 2014).

absorbed many of the functions previously held by various federal entities such as the National Infrastructure Protection Center of the Federal Bureau of Investigation and the National Communications System (NCS) of the Department of Defense. The National Communications System (NCS) was an interagency organization initially established in 1963, and re-chartered by Executive Order 12472 in April 1984, to assist the Executive Office of the President in exercising wartime and non-wartime emergency telecommunications responsibilities. The mission of the NCS was to coordinate the planning for and provisioning of national security and emergency preparedness communications for the Federal Government under all circumstances. The NCS consisted of the telecommunications assets of twenty-three Federal departments and agencies. The primary mission of DHS is to prevent terrorist attacks within the U.S., reduce the vulnerability of said attacks, and minimize the damage, and assist in the recovery.[105] The Homeland Security Act established a Directorate for Information Analysis and Infrastructure Protection, which is charged with assessing the vulnerabilities of the key resources and critical infrastructure of the United States. The Directorate establishes under paragraph 14, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure.[106]

Federal regulation establishes the Department of Homeland Security (DHS) as the focal point for the security of cyber space-including recovery efforts for public and private critical infrastructure systems.[107] DHS is the federal agency charged with providing physical security, primarily through the National Cyber Security Division (NCSD). The NCSD is tasked with

[105]107th U.S. Congress, "Public Law 107-296" (U.S. Government, November 25, 2002), http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed January 13, 2014).

[106]107th U.S. Congress, "Public Law 107-296" (U.S. Government, November 25, 2002), http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed January 13, 2014).

[107]Wilshusen, *GAO-08-212T Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, 1.

developing an integrated public/private plan for Internet recovery. Their federal-civilian partnership with the Information Technology Sector Coordinating Council (IT SCC) share a commitment of improving the security of critical technology infrastructures.[108] There is no federal authority over the council, and the private sector is considered a partner in the interest of national security. The stated objectives are accurate but subservient to the proprietary nature of the private sector. Physical security requirements are not standardized at the federal level, but instead rely upon a loose set of industry standards where interpretation and cost considerations play a role.[109]

Additionally, key legislation on cyber infrastructure protection does not address roles and responsibilities in the event of a disruption nor have existing laws been validated in the event of an actual cyber emergency.[110] The past three Presidential administrations have adhered to the similar strategy of private and governmental partnership in lieu of explicit federal oversight.[111] This strategy meant to promote the economic advantages of cyberspace while encouraging network security. The 2011 DoD Strategy for Operating in Cyberspace highlight the use of cyberspace in terms that reflect American principles: an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and social networks that energize the economy.[112]

In February 2013, the President issued Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, which explicitly calls for an update to the National

---

[108]Department of Homeland Security, "Information Technology Sector-Specific Plan An Annex to the National Infrastructure Protection Plan" (Department of Homeland Security, 2010), 3.

[109]Ibid.

[110]Wilshusen, *GAO-08-212T Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*."

[111]Martin, Jr., "Paradigm Change: Cybersecurity of Critical Infrastructure," 39.

[112]Department of Defense, "Department of Defense: Strategy for Operating in Cyberspace," 1.

Infrastructure Protection Plan (NIPP).[113] The NIPP meets the requirements that the President set forth in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection.[114] The 2013 National Plan builds upon previous NIPPs by emphasizing the complementary goals of security and resilience for critical infrastructure. To achieve these goals, cyber and physical security and the resilience of critical infrastructure assets, systems, and networks are integrated into an enterprise approach to risk management.[115] Released February 12, 2013, PPD-21 was written to advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.[116] This update is informed by significant evolution in the critical infrastructure risk, policy, and operating environments, as well as experience gained and lessons learned since the NIPP was last issued in 2009.

The National Strategy to Secure Cyberspace, HSPD-7, NSPD-54/HSPD-23, and the Homeland Security Act identify the responsibilities of the various CIKR partners with a role in securing cyberspace.[117] One of the 2013 NIPP's key concepts is the greater focus on integration of cyber and physical security efforts. The National Infrastructure Protection Plan (NIPP) is the

[113]Department of Homeland Security, "National Infrastructure Protection Plan Fact Sheet" (Department of Homeland Security, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 18, 2014).

[114]Department of Homeland Security, "NIPP 2013: Partnering Critical Infrastructure Security and Resilence", 2103, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf (accessed January 21, 2014).

[115] Department of Homeland Security, "NIPP 2013: Partnering Critical Infrastructure Security and Resilence", 2103, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf (accessed January 21, 2014).

[116]The White House, "Presidential Policy Directive 21" (The White House, February 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 12, 2014).

[117]"National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency" (Department of Homeland Security, 2009), 114, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed January 6, 2013).

DHS framework to protect U.S. critical infrastructure and key resources (CIKR) from man-made and naturally occurring threats.[118] NIPP 2013 was developed through a collaborative process that included the active participation of the critical infrastructure community, including private industry; public and private sector owners and operators; State, local, tribal, and territorial government agencies; non-governmental organizations; Sector-Specific Agencies; and other Federal departments and agencies.[119] Initially introduced in 2006, the NIPP outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. The U.S. Department of Homeland Security (DHS) released the National Infrastructure Protection Plan (NIPP) in 2006 to serve as a comprehensive risk management framework and address the preexisting threat environment of natural disasters, cyber attacks, and terrorism. The NIPP has since been updated and further defines critical infrastructure protection roles and responsibilities for all levels of government and private industry. DHS recognizes that a successful risk assessment framework requires cooperation and coordination among Federal departments and agencies; State, local, and tribal governments; private sector owners and operators; and international partners.[120]

The 2010 Communications Sector Specific Plan (CSSP) addresses the critical communications infrastructure security issue. The U.S. Department of Homeland Security (DHS), National Communications System (NCS) serves as the Sector-Specific Agency for the Communications Sector. Private sector owners and operators have enjoyed a close working

[118]Department of Homeland Security, "NIPP 2013: Partnering Critical Infrastructure Security and Resilence."

[119]Ibid., i.

[120]Department of Homeland Security, "2010 Communications Sector-Specific Plan" (Department of Homeland Security, 2010), 1, http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf (accessed January 18, 2014).

relationship with NCS since its inception in 1963.[121] The CSSP is the result of close collaboration among NCS, the Communications Sector Coordinating Council, and the Communications Government Coordinating Council. It provides a framework through which industry and government partners can develop a coordinated protection strategy.[122] In addition to conducting risk assessments of critical infrastructure, the CSSP Sector partners placed a new emphasis on interdependencies, partnerships, coordination, and collaboration among all levels of government and with the private sector.[123] To implement the NIPP, Sector-Specific Agencies (SSAs) for each of the 18 critical infrastructure and key resources (CIKR) sectors are partnering with State, local, and tribal governments, and industry to create and implement Sector-Specific Plans (SSPs). The DHS National Communications System (NCS) serves as the SSA for the Communications Sector. NCS and its partners coordinate the development of the Communications SSP (CSSP) to reduce risk across the Communications Sector. The CSSP is intended to ensure that the Communications Sector effectively coordinates with sector partners, other sectors, and DHS to enhance protection and resilience in an all-hazards environment. The CSSP presents a vision of how the Communications Sector will manage risk utilizing both public and private resources, how partners will implement programs and practices to achieve sector goals, and how the sector will measure the success of protective activities.[124]

The Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the

[121]Department of Homeland Security, "2010 Communications Sector-Specific Plan."

[122]Department of Homeland Security, "2010 Communications Sector-Specific Plan.", v.

[123]Department of Homeland Security, "2010 Communications Sector-Specific Plan.", 1.

[124]Department of Homeland Security, "2010 Communications Sector-Specific Plan," 1.

economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.

Phyllis Schneck, the deputy undersecretary for cybersecurity at the DHS' National Protections and Programs directorate, has outlined a new plan that capitalizes on President Obama Executive Order (EO) 13636 signed in February 2013.[125] EO 13636, issued in conjuction with Presidential Policy Directive-21(PPD-21): Critical Infrastructure Security and Resilience, replaces HSPD-7 and directs the DHS to explore voluntary programs for private and public entities to participate together to increase cybersecurity awareness as well as promulgate best practices from the cyber industry.[126] PPD-21comes on the heels of PPD-20, the Executive Order signed in November 2012 that establishes a broad and strict set of standards to guide the operations of federal agencies in confronting threats in cyberspace.[127] PPD-20 goes further to define what constitutes offensive and defensive actions and outlines what role federal authorities

[125]Jason Miller, "DHS Revs up Its Part of the Cyber Executive Order," *Federal News Radio*, last modified January 31, 2014, http://www.federalnewsradio.com/?nid=473&sid=3553526&pid=0&page=1 (accessed February 6, 2014).

[126]Jason Miller, "DHS Revs up Its Part of the Cyber Executive Order," *Federal News Radio*, last modified January 31, 2014, http://www.federalnewsradio.com/?nid=473&sid=3553526&pid=0&page=1 (accessed February 6, 2014).

[127]Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks," *The Washington Post*, last modified November 2012, http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html (accessed February 6, 2014).

and the military will take in the domains of "network defense" and "cyber-operations".[128] These measures are steps in the right direction, providing more detail on roles and responsibilities.

This government framework has been exercised, most recently during the spring of 2012.[129] The largest banks in the United States were under cyber attack with hackers commandeering servers around the world to direct a barrage of Internet traffic toward the banks' websites.[130] The attacks were privately attributed to Iran, and instead of confronting or counterattacking the perceived source, the Department of Homeland Security and their partners tried a new approach. They applied the private-public partnership model with global allies to confine the attacks and basically restrict their access to the banks' servers. The result was a reduction in DDoS traffic but not a complete elimination of attacks. Although some argued that the response was not aggressive enough, it did build confidence among DHS and their partners and reaffirmed the public-private model.[131]

Submarine Cables

Submarine cables have been in existence since the 1820's. Centered on telegraphy, the cables served the purpose of connecting countries around the globe. The first trans-Atlantic cable was laid in 1858 between Ireland and Newfoundland with a substantial reduction in transmission

[128]Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks."

[129]Ellen Nakashima, "U.S. Rallied 120 Nations in Response to 2012 Cyberattack on American Banks," *Washington Post*, April 11, 2014, http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html (accessed April 22, 2014).

[130]Ellen Nakashima, "U.S. Rallied 120 Nations in Response to 2012 Cyberattack on American Banks," Washington Post, April 11, 2014, http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html (accessed April 22, 2014).

[131] Nakashima, "U.S. Rallied 120 Nations in Response to 2012 Cyberattack on American Banks."

time and costs.[132] By the early 20th century, much of the world was connected by a network that enabled rapid communication and dissemination of information for government, commerce and the public. The invention of invention of repeaters in the 1940s and their use in TAT-1, the first transatlantic telephone cable, began an era of rapid and reliable transoceanic communications.[133] The next major advancement was the first international fiber-optic cable in 1986 that connected Belgium to the UK.[134] This marked a huge increase in capacity, with 40,000 simultaneous phone calls, ten times that of the last copper-based telephone cable.[135] By 1988 fiber-optic technology replaced the original copper based wires, and the new technology complimented the Internet by enabling large volumes of voice and data traffic to be rapidly carried around the globe.[136] TAT-8, a project led by AT&T, BT, and France Telecom, became the first transoceanic fiber-optic cable to be installed.[137]

The cyber dot-com bubble of the late 1990's followed, with millions of miles of cable laid in order to meet demands for more bandwidth the Internet required.[138]

---

[132]Lionel Carter et al., "Submarine Cables and the Oceans – Connecting the World" (UNEP-WCMC Biodiversity Series, 2009), 13, http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf (accessed March 6, 2014).

[133]"About Submarine Telecommunications Cables" (International Cable Protection Committee, October 2011), 4, http://www.iscpc.org/publications/About_SubTel_Cables_2011.pdf (accessed March 8, 2014).

[134]"About Submarine Telecommunications Cables" (International Cable Protection Committee, October 2011), 4, http://www.iscpc.org/publications/About_SubTel_Cables_2011.pdf (accessed March 8, 2014).

[135]Ibid., 5.

[136]Mick Green et al., "Submarine Network Security" (International Cable Protection Committee, April 13, 2009), 6.

[137]Capt (R) Douglas R. Burnett, Submarine Cables: Critical Infrastructure (Squire Sanders Legal Counsel Worldwide, May 20, 2012), 6, www.virginia.edu/colp/pdf/Burnett-Presentation.pdf (accessed February 28, 2014).

[138]Anton Troianovski, "Optical Delusion? Fiber Booms Again, Despite Bust," *The Wall Street Journal*, April 3, 2012, http://online.wsj.com/news/articles/SB10001424052702303863404577285260615058538 (accessed March 8, 2014).

The exponential growth in the Internet found its way overseas via existing underwater telecommunication cables. Undersea cables account for 95% of the world's international voice and data traffic while satellites account for less than 5%.[139] This overwhelming amount of U.S. international internet communications depend upon about 35 international cables, each the size of a garden hose.[140] The vulnerability inherent in such as small amount of cables carrying the majority of sensitive U.S. economic and security information amplifies the importance of securing these cables from unauthorized intrusion. Historical trends as well as recent events indicate that breaking submarine cables pose a legitimate threat to the security of cyber infrastructure.

The telecommunications network has morphed into the Internet, and with it a vast physical infrastructure that retains the complexity and vulnerability of its predecessor.[141] The vast network of submarine fiber-optic cables that crisscross the ocean floor require constant maintenance just from natural and accidental occurrences. Countries that derive their access to the global information grid from one or two cables could be without access if the incident was severe enough. The December 19, 2008 outage in the Mediterranean Sea highlight this situation. The Middle East and parts of Southeast Asia experienced network degradation, with Egypt losing as much as 80% of their network.[142] The limited amount of access points in third-world countries could easily see another scenario like this one.

The 2007 Vietnamese incident highlight another example where security measures failed on the most basic of levels. Vietnamese fisherman pulled up 500 kilometers of operational cable

---

[139]Capt (R) Douglas R. Burnett, "Cable Vision," *Proceedings*, August 2011, http://www.usni.org/magazines/proceedings/2011-08/cable-vision (accessed February 28, 2014).

[140]Burnett, "Submarine Cables: Critical Infrastructure."

[141]Geary, "Who Protects the Internet?," 52.

[142] Geary, "Who Protects the Internet?," 50.

with the hopes of selling it on the black market.[143] Vietnam was reduced to routing the majority of its Internet traffic over one cable line and satellite links, causing substantial delays for three months and over 5.8 million in damage.[144] The Prime Minister of Vietnam said the theft "directly affects Vietnam's socio-economic development, national security and the country's prestige in the region as well as in the world."[145]

One of the underlying assumptions in regards to submarine cables is that the natural vastness of the ocean would provide security from human intervention, either accidently or nefariously. Throughout the 19th and early 20th century, most of the ocean was unaffected by human interaction outside of shipping and regional fishing.[146] Globalization has helped bring about a change by connecting those previously isolated due to geographical or ideological reasons. Human activities, directly or indirectly, have affected and altered all environments world-wide, including the 71 per cent of the planet that is ocean. The number and the intensity of maritime uses have increased dramatically and will continue to do so in the future, stretching the capacity of the oceans and their finite Submarine cable present numerous security problems. Information on the 500,000 undersea cables are open-source information for the commercial professions such as mariners and fishermen.[147] The lack of international law has made enforcement of illegal action such as pirate activity next to impossible. Where international law does exists, third-world countries are unprepared to enforce the regulations.

---

[143]Michael Sechrist, "Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership" (Harvard Kennedy School, March 23, 2010), 42, http://belfercenter.hks.harvard.edu/files/PAE_final_draft_-_043010.pdf (accessed March 9, 2014).

[144]Burnett, Submarine Cables: Critical Infrastructure, 24.

[145]Jacqui Cheng, "Phishing Plumbs New Depths: Vietnamese Fishermen Sever Fiber Optic Lines," *Arstechnica*, last modified June 8, 2007, http://arstechnica.com/uncategorized/2007/06/phishing-plumbs-new-depths-vietnamese-fishermen-sever-fiber-optic-lines/ (accessed March 9, 2014).

[146]Carter et al., Submarine Cables and the Oceans – Connecting the World," 3.

[147]Geary, "Who Protects the Internet?," 49.

Access to Top Secret/Sensitive Compartmented Information (TS/SCI) networks can be accessed via the same fiber optic networks and other privatized hardware.[148] DoD and U.S. intelligence agencies utilize the same hardware as the public Internet, and traverse the same cables as commercial providers.[149] For example, the NSA utilizes the "Upstream Program", a collection program on fiber cables and infrastructure that transports 95% of all internet traffic in the U.S.[150] This becomes complicated when the biggest operators of those cables was sold to an Asian firm, potentially complicating American surveillance efforts.[151] The U.S. government has implicated control measures in the way of approving cable licenses via the Federal Communications Commission.[152] A group of lawyers dubbed "Team Telecon" representing the DoD, DHS, and the FBI have developed security agreements that went beyond what's required by the laws governing electronic eavesdropping.[153] This brings into question of vulnerability. Our enemies, for strategic or operational reasons, would target the physical infrastructure that pass information for terrorists groups such as Al Qaeda.

---

[148]Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do about It*, 1st ed. (New York: Ecco, 2010), 173.

[149]Ibid., 183.

[150]Craig Timberg, "NSA Slides Explain the PRISM Data-Collection Program," *Washington Post*, July 10, 2013 , http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html, (accessed November 1, 2013).

[151]Craig Timberg and Ellen Nakashima, "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance," *Washington Post*, July 10, 2013, http://www.washingtonpost.com /business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html (accessed November 1, 2013).

[152]Ibid.

[153]Craig Timberg and Ellen Nakashima, "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance," *Washington Post*, July 10, 2013, http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html (accessed November 1, 2013).

The lack of an overarching governing authority makes the cables a vulnerability terrorist could exploit with minimal operational risk. Submarine cables are covered by the United Nations Convention on Law of the Sea (UNCLOS), signed December 10, 1982 and ratified on November 16, 1994 by 166 parties, with the notable exception of the United States.[154] Ongoing debate in the U.S. Senate over the treaty's perceived erosion of U.S. sovereignty, both in terms of international arbitration of disputes and the possibility that a supranational body could impose binding rulings on the U.S. [155] The United States could block some but not all actions of the International Seabed Authority, a legislative body vested with significant power over more than half of the earth's surface.[156] UNCLOS followed previous laws such as the International Convention for the Protection of Submarine Cables (1884) and the Geneva Conventions of the Continental Shelf and High Seas (1958).[157]

James Lewis, Center of Strategic and International Studies (CSIS) director, says "During the Cold War, lots of attention was paid to undersea cables."[158] Submarine cables can be the single points of failure in a system full of redundancies. Scenarios such as the 2007 Vietnamese pirate incident, 2009 Somali, and the 2013 Egypt all substantiate the claim that cables can create sustained delays due to authority conflicts and repair timelines. Syria and Ukraine, countries in current headlines due to civil unrest, both share similar vulnerabilities when it comes to cyber

[154]Carter et al., "Submarine Cables and the Oceans – Connecting the World," 26.

[155]Keith Johnson, "GOP Scuttles Law-of-Sea Treaty," *The Wall Street Journal*, July 16, 2012, http://blogs.wsj.com/washwire/2012/07/16/gop-opposition-scuttles-law-of-sea-treaty/ (accessed March 14, 2014).

[156]"Senators Portman and Ayotte Sink Law Of The Sea Treaty," *Rob Portman, United States Senator for Ohio*, last modified July 16, 2012, http://www.portman.senate.gov/public/index.cfm/press-releases?ID=a886f01e-1b08-4c51-bf7e-4bad33194c0b (accessed March 6, 2014).

[157]About Submarine Telecommunications Cables, 24.

[158]Geary, "Who Protects the Internet?," 54.

infrastructure. The United States was reportedly considering the use of cyber attack to disable the Syrian cyber infrastructure with Russia postured to the do the same in the Ukraine.[159]

Empirical

Colin Gray's recently published Strategic Studies Institute report makes the case that cyber power is not a strategic vulnerability and does not pose a challenge to the theory of strategy.[160] Gray argues that cyber is the next great intellectual challenge, similar to strategic bombing and nuclear war. He states that while cyber is a revolution in military affairs, it should be considered in terms of geography and information. When compared to land power, sea power, airpower, and space power, cyber power has its own "grammar" described by Clausewitz. Gray draws four conclusions to support his argument. First, Gray refutes that assumption that stand-alone cyber attacks will prove catastrophic. Any cyber attack can be quickly recovered from. Secondly, cyber attacks will not possess the lethality necessary to be catastrophic. He argues that cyber attacks will be instantaneous, but defenses will be adequate to prohibit critical damage. Third, cyber concerns information, which Gray argues is not critical to strategic success. Fourth, and most importantly, the cyber "9-11" scenarios will not occur due to strategic constraints emplaced by both sides.

Gray's argument conveniently omits the physical infrastructure and the human element behind cyber power. The absence of "meaningful physicality" of cyberspace relegates it to just another means of waging war. Gray references Clausewitz in that war's political aims must adapt to the means available. Cyber power, along with air and nuclear power, is just another means to

[159]Kevin G. Coleman, "Syria and Ukraine Share Cyber Vulnerabilities," *C4ISR & Networks*, last modified March 3, 2014, http://www.c4isrnet.com/article/M5/20140303/C4ISRNET18/303030009/Syria-Ukraine-share-cyber-vulnerabilities (accessed March 8, 2014).

[160]Gray, Army War College (U.S.), and Strategic Studies Institute, *Making Strategic Sense of Cyber Power Why the Sky Is Not Falling*, vii.

accomplishing the ends. Unlike those tangible domains, however, cyber is something that is defined by both protagonists. Gray repeatedly makes the case that cyber can be grouped into the same category strategically as air or nuclear, with strategic deterrents inherent to the employment of any offensive capability. Gray argument essentially states that although an attack is possible, it certainly doesn't make sense strategically for state actors due to the reciprocal nature.

James A. Lewis suggests that computer network vulnerabilities are an increasingly serious business problem but that their threat to national security is overstated as well.[161] Lewis addresses the threat as cyber-terrorism and defines it as "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[162] The premise of cyber terrorism is that as nations and critical infrastructure became more dependent on computer networks for their operation, new vulnerabilities are created – "a massive electronic Achilles' heel." Lewis cites enduring historical strategies such as Douhet's aerial bombing in World War I or the U.S. strategic bombing of World War II that emphasized attacks on critical civil infrastructures, each failing to produce the desired effect.[163]

Lewis argues critical infrastructures, especially in large market economies, are more distributed, diverse, redundant and self-healing than a cursory assessment may suggest, rendering them less vulnerable to attack.[164] He cites the system failures and outages of U.S. infrastructure that currently exist that doesn't affect national security. On a national level, where dozens or even hundreds of different systems provide critical infrastructure services, failure is a routine

[161]James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats" (Center for Strategic and International Studies, 2002), 2.

[162]Ibid., 2.

[163]Ibid., 3.

[164]James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats" (Center for Strategic and International Studies, 2002), 2.

occurrence at the system or regional level, with service denied to customers for hours or days.[165] Cyber-terrorists would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or to have any noticeable effect.[166] For most of the critical infrastructure, multiple sustained attacks are not a feasible scenario for hackers, terrorist groups or nation states. Lewis references the risk of discovery as a deterrent for nation states from attacking cyber infrastructure, which leaves proxy actors as the likely candidate to execute attacks and they are not equipped to execute such prolonged attacks.

Richard A Clarke takes a different perspective to cyber warfare. Clarke asserts that cyber is the next threat to national security and that now is the time to discuss what U.S. cyber strategy should encompass, similar to those discussions held at the beginning of the nuclear age.[167] Clarke sites the shortcomings of the U.S. cyber strategy and the lack of overall authority by its lead cyber defense agency, U.S. Cyber Command. US CYBERCOM's mission is to defend the Department of Defense but not the critical infrastructure. This includes the cyber infrastructure.[168] Former NSA Director Ken Minihan argues that the DoD would not be able to defend the U.S. from a cyber attack.[169] DHS defends only the non-DoD part of the federal government. As Clarke writes, "there is no federal agency that has the mission to defend the internet infrastructure.[170] The last three U.S. Presidents have followed that approach, with DHS and DoD protecting only the federal sector of the internet. Clarke proposes his "Defensive Triad" strategy to correct this and the first target is the internet infrastructure. The large ISPs (AT&T, Verizon, Level 3, Qwest,

[165]Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats."

[166]Ibid.

[167]Clarke, *Cyber War*, x.

[168]Ibid., 43.

[169] Clarke, *Cyber War*, x.

[170]Ibid., 143.

and Sprint), own the majority of the fiber-optic cable that runs across the country. His intent is to use federal regulation to impose cyber security requirements.[171] These companies run the "trunks" or Tier 1 ISPs, which can connect to the majority of other ISPs in the country. These are the companies that own the thousands of miles of fiber-optic cable that span the country as well as the undersea fiber-optic cables around the world.[172] DHS has adopted a strategy of shared responsibility in order to divert costs and keep the internet an open network. Similar to the conflict of national interest in the military industrial complex, this strategy has led to private industry interest taking priority over comprehensive security measures adhered to by all.

Summary

Cyber infrastructure physical vulnerability has been relegated to the background of the cyber warfare discussion. The very high damage potential of an attack is countered by the low risk of occurrence and regulates the threat to the domain of a black swan event. Associated with the other CIKR sectors, cyber infrastructure physical vulnerability has been dismissed in favor of the virtual attack that has materialized to limited effect. Although cyber has been has added as the fifth warfighting domain, it does not qualify as a RMA. This limits its strategic effect and therefore marginalizes its value as an operational target for our enemies. Empirical studies are divergent, ranging from "the sky is not falling" approach to the more technical theory that existing terrestrial infrastructure contain single points of failure and thus provide an interconnected target that could cripple a large amount of our automated systems. The private-public partnership reveals a system without adequate regulation in place as well as a reliance on private industry to provide security for infrastructure that is utilized by government agencies.

---

[171] Richard A. Clarke, *Cyber War: The next Threat to National Security and What to Do about It*, 1st ed. (New York: Ecco, 2010), 160.

[172] Ibid.

The absence of a coherent strategic defensive theory, coupled with the lack of a codified single authority reveal gaps in a comprehensive security plan. The failure of DHS to get all the private partners to agree on security standards and the vagueness of DoD's infrastructure security mission compound the issue. The cyber threat (virtual and physical) have been conveniently consolidated together and much remains to be analyzed in terms of actual physical vulnerability. Cyber infrastructure vulnerability will remain a threat as long as it is regulated to the background of the discussion of cyber warfare as a whole.

METHODOLOGY

This study will utilize a scenario-based qualitative approach to focus on the physical characteristics of the cyber infrastructure, the private-public partnership, authority and regulations. The scenarios will incorporate the strategic theories associated with cyber infrastructure, the failure of legislation to institute applicable security regulations, the lack of private industry defensive measures, and the status of cyber infrastructure authority statues. The theory will predict that the absence of a coherent and inclusive cyber infrastructure defensive strategy increase the vulnerability of cyber infrastructure to physical attack and decrease access. The scenarios will address the range of security and Internet access on the private-public continuum as well as the risk of the threat involved. They will also address the possibility of limited access to the Internet and the impact to various financial and government entities. This research creates variable outcomes that will address the current lapses in cyber infrastructure legislation and the command and control discrepancies of having multiple agencies in charge of multiple domains.

The scenarios will incorporate the Army Design Methodology (ADM) and Military Decision Making Process (MDMP) assessment with courses of action to best assure continue Internet access. The operational approach will focus on authority, regulations, and security as

lines of effort. The courses of action will center on defense-in-depth and deterrence. This operational approach will show how thinking about cyber infrastructure integrates with overall planning.

Scenario planning derives from the observation that, given the impossibility of knowing precisely how the future will play out, a good decision or strategy to adopt is one that plays out well across several possible futures.[173] There has been a limited amount of documented attacks against cyber infrastructure, as the CSIS study referenced earlier determined. That being the case, multiple and divergent scenarios that model a distinct, plausible operating environment will help in determining the appropriate strategy to select in protecting cyber infrastructure.[174] To find that "robust" strategy, scenarios are created in plural, such that each scenario diverges markedly from the others. These sets of scenarios are, essentially, specially constructed narratives about the future, each one modeling a distinct, plausible environment to plan against.[175]

Peter Swartz simplified the scenario process by breaking down the methodology to five steps.[176] The five steps are list driving forces, make a scenario grid, imagine possible futures, brainstorm implications and actions, and track indicators. This is a revision of his earlier work, which expanded the list to include selecting and fleshing out scenario logics and segmenting driving forces into "predetermined" and "highly uncertain."

SCENARIOS

[173]Lawrence Wilkinson, "How to Build Scenarios Planning for 'Long Fuse, Big Bang' Problems in an Era of Uncertainty," *Wired*, 1995, http://www.wired.com/wired/scenarios/build.html (accessed March 26, 2014).

[174]Ibid, 1.

[175]Ibid., 1.

[176]Peter Schwartz, *The Art of the Long View*, 1st ed. (New York: Doubleday/Currency, 1991), 226.

This study will forecast eight scenarios. The scenarios will describe the relationships between actor (state vs non-state), severity (simple vs complex), and recovery (slow vs fast) of potential cyber infrastructure attacks. Figure 1 depicts the eight scenarios in a cube graphic.

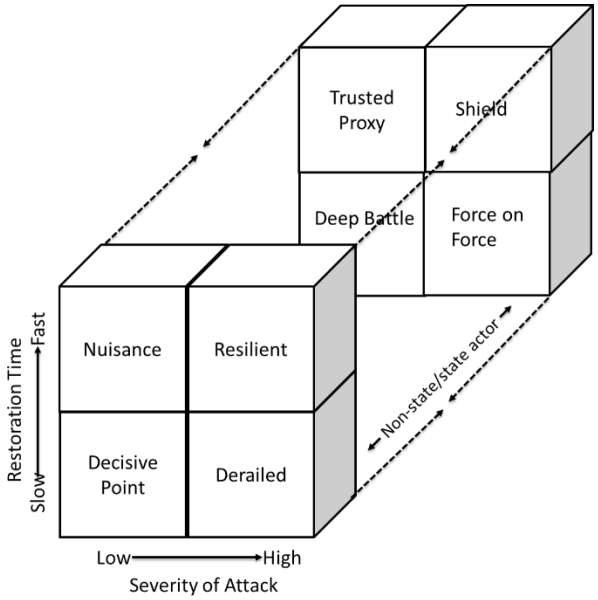

Figure 1. Cyber infrastructure scenarios

The first four scenarios will look at infrastructure security and non-state actors and the other four scenarios will look at infrastructure security and state actors. The scenarios were selected based on current trends. The first trend is infrastructure access. Recent events such as the 2008 Egypt submarine cable cut highlight what could occur to Internet access when just one main cable is cut. Non-state actors such as Somalia pirates or even fisherman, as was the case in that instance, can cause substantial damage to the infrastructure and cause an outage that lasts an extended amount of time.

The other four scenarios will be based on infrastructure security and state actors. These scenarios will look at what might occur if the threat was upgraded with the capabilities a state actor brings to the table. These scenarios will envision a coordinated attack where not only is the

physical infrastructure attacked but is superseded by a virtual cyber attack as well, rendering the network inoperable and access degraded for an extended period of time. These scenarios will represent the "Black Swan" event that could occur if a state actor were able to bring to bear the capability they currently possess.[177]

Driving Forces

The first step to Peter Swartz's methodology in developing scenarios (after identifying the focal issue) is to determine the key and driving forces behind the issue. Micro and macro environments can organize the issues. The micro environment consists of actors or decision makers behind the focal issue. Central to this arena are the local influences and considerations that make up the identity of the key actors. The macro environment consists of the "driving" trends that form the contextual environment. This "inside/outside" approach helps understand the indirect contextual environment as well as the direct contextual environment where decisions are made by the key actors.

The driving forces for the eight scenarios are depicted in Figure 1 below.

[177]Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed., Random trade pbk. ed. (New York: Random House Trade Paperbacks, 2010). Taleb describes the low probability, high impacts of "Black Swan" events.

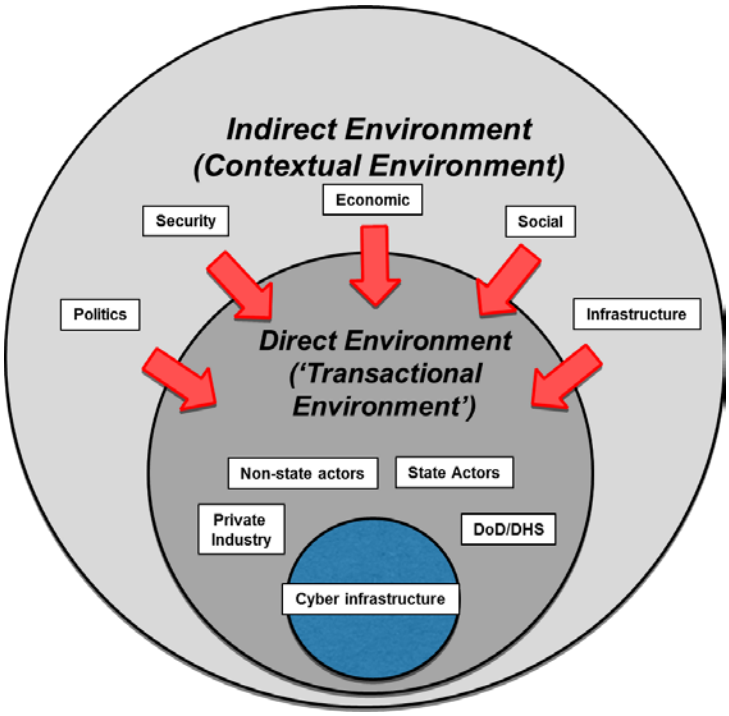

Figure 1. Cyber Infrastructure driving forces

The contextual environment consists of elements commonly referred to PMESII-PT (Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time).[178] The scenarios will assume the same contextual environment. For the purposes of the exercise, the relevant variables will be politics, military (security), economic, social, and infrastructure.

The political conditions are characterized by the changing international distribution of power, decline of global governance, and shortfalls in state governance. The changing international distribution of power is a result of the collapse of the Soviet Union. The bipolarity of the Cold War has been replaced by the multi-polarity of ascending states to fill the power

[178]Headquarters, Department of the Army, *Operational Environments to 2028: The Strategic Environment for Unified Land Operations* (Training and Doctrine Command, August 2012), 2, http://www.arcic.army.mil/app_Documents/ TRADOC_Paper_Operational-Environments-to-2028-Strategic-Environment-for-Unified-Land-Operations_AUG2012.pdf (accessed March 28, 2014).

vacuum. Nuclear weapons proliferation was limited to the two main protagonists, and the strategy of deterrence was adopted. Both options and limits were considered in the context of an overarching strategic view based on a broad consensus.[179] John Mearsheimer argues that multi-polarity is the cause of instability as the imbalance of power leads states to go unchecked in an attempt to counteract their adversaries' actions.[180] Global governance, defined as the collective management of common problems at the international level will likely decrease due to increasing numbers and influence of non-state actors.[181] Using multipolarity as the predominant power arrangement, states and non-state actor alike will resort to resort to regional solution to address collective problems, without considering the impact to the whole.[182] Shortfalls in state governance refers to the challenges many failing states have in maintaining political legitimacy due to the lack of institutional, infrastructural, human, and material resources required to provide for basic needs.[183] A closer look at the U.S. perspective shows the difficulty past administrations have had in getting needed legislations passed in Congress. The tensions inherent with the private-public partnership describe the situation where infrastructure proprietors have the responsibility of securing cyber infrastructure, and the public trust is dependent on market forces.[184]

---

[179]Headquarters, Department of the Army, *Operational Environments to 2028: The Strategic Environment for Unified Land Operations* (Training and Doctrine Command, August 2012), 13, http://www.arcic.army.mil/app_Documents /TRADOC_Paper_Operational-Environments-to-2028-Strategic-Environment-for-Unified-Land-Operations_AUG2012.pdf (accessed March 28, 2014)..

[180]John Mearsheimer, "Back to the Future," *International Security* 15, no. 1 (Summer 1990): 14, accessed March 28, 2014, http://www.jstor.org/stable/2538981.

[181]*Operational Environments to 2028: The Strategic Environment for Unified Land Operations,* 15.

[182]Ibid.

[183]Ibid., 16.

[184]Martin, Jr., "Paradigm Change: Cybersecurity of Critical Infrastructure," 43.

The security environment will consist of a networks of adversaries with a wide range of sophistication, capabilities, and goals.[185] The range of threats include criminal organizations, terrorists, states and non-state actors, insurgents, transnational groups, proxies, technologically-empowered individuals, and paramilitaries.[186] These actors have various motivations that provide challenges to planners in developing comprehensive security measures. The multipolarity of threat, coupled with the numerous access points to the infrastructure, increase the level of risk. The risk to mission is high as a static defense will eventually yield under constant attack.[187] Additionally, non-state actors and unconventional operational methods will blur the lines between civilian law enforcement and the military.[188] This tension is directly applicable to the cyber infrastructure issue as authority has been spread across multiple agencies, each with their own domain.[189] One of the areas where the threat will operate is the global commons. As just one example of current attacks in the cyberspace common, external sources—both governmental and non-state actors—are working daily to penetrate U.S. DOD networks, and foreign intelligence organizations have acquired the capacity to disrupt the U.S. military's information infrastructure.[190] The overlapping mission sets result in ambiguity in terms of emergency preparedness.[191]

---

[185]Headquarters, Department of the Army, *Operational Environments to 2028: The Strategic Environment for Unified Land Operations*, 17.

[186]Ibid, 17.

[187]Clausewitz, *On War*.

[188]*Operational Environments to 2028: The Strategic Environment for Unified Land Operations*, 15.

[189]Thomas Goss, "'Who's in Charge?' New Challenges in Homeland Defense and Homeland Security," *Homeland Security Affairs* II, no. 2 (2006): 8, http://www.hsaj.org/?fullarticle=2.1.2 (accessed March 28, 2014).

[190]Headquarters, Department of the Army, *Operational Environments to 2028: The Strategic Environment for Unified Land Operations*, 19.

[191]Goss, "'Who's in Charge?' New Challenges in Homeland Defense and Homeland Security," 5.

The economic situation depicts the shift in wealth from western to eastern states and the rise of non-state actors and criminal organizations.[192] The alliance of the latter demonstrates the increasing influence of non-state actors as an agent for change on the global stage. Globalization, the interconnectness and resulting interdependence of the global economy highlight the importance of cyber infrastructure in providing the networks necessary to keep the global markets intact. Disruptions risk propelling once-isolated local events into potentially catastrophic global events.[193]

The social component of cyber infrastructure is readily apparent in the day to day lives of the world population. As our lives becomes more dependent on technology, the demand for instantaneous and uninterrupted access will only increase. Even small outages can have repercussions depending on the length of disruption could impact not only social aspects but financial markets as well.[194] The risk of non-state actors and criminal organizations using this vulnerability to impact their adversaries is high, considering the risk versus reward involved.

Infrastructure growth in developed and developing countries, coupled with urbanization of most of the world, will drive cyber infrastructure dependency and therefore increase the security risk. As the Internet becomes more prevalent in the third world countries, regions rife with ideological beliefs and regional conflict where denial of service will be a tactic to silence opposing views. The fact that most of the cyber infrastructure is unsecured will serve as a soft target for those with limited resources and capability. The impact and notoriety that comes with

[192]Department of the Army, "Operational Environments to 2028: The Strategic Environment for Unified Land Operations," 20.

[193]Ibid., 21.

[194]Eric Mack, "Google Outage Reportedly Caused Big Drop in Global Traffic," *CNET*, last modified August 2013, http://www.cnet.com/news/google-outage-reportedly-caused-big-drop-in-global-traffic/ (accessed March 28, 2014).

disrupting a global network will only further non-state and criminal actors' agenda and result in a loss in confidence in the system as a whole.

Non-State Actors and Criminal Scenarios

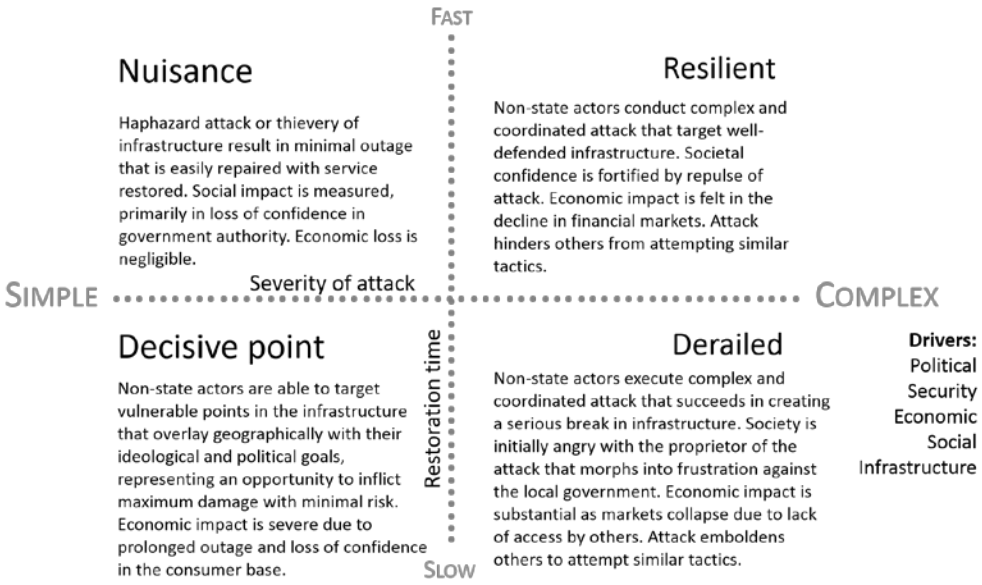

Figure 2. Non-state actor and criminal scenarios

The first fours scenarios will look at non-state actors and criminals and infrastructure access. Figure 1.2 depicts these scenarios in a quadrant graphic. The horizontal access labeled "severity of attack" characterizes the scale of attack that could occur given the capabilities of non-stop actors and criminal organizations. The vertical axis represents the level of Internet access. The four quadrants provide a narrative of the probable scenario.

"Nuisance" describes a scenario where an attack or theft of infrastructure results in an outage that is restored with a minimal amount of down time in network services. This scenario describes the majority of perceived attacks and outages that have occurred to cyber infrastructure such as submarine cables. This scenario could describe the 2008 Middle East incident that

affected Egypt and India.[195] Although the actual cause was never fully determined, and the cuts resulted in outages to a large portion of the region, access was restored in relatively short amount of time.[196] These attacks could be easily dismissed, however, the success in creating an extended outage will not go unnoticed by those who seek to learn where the vulnerabilities in the network are. The outages in Egypt and India could be capitalized on by political adversaries of those countries who want to cause social unrest and create turbulence in existing political systems.

The second scenario, "Decisive Point", describes a scenario where non-state actors are able to target infrastructure and create an outage that affects a large geographical area for an extended period of time. This would be characterized by the March 2011 intentional attack off the coast of Alexandria, Egypt.[197] Three divers intentionally cut through the SeaMeWe-4 submarine cable, affecting not only Egypt but Europe and Africa as well.[198] The divers were able to find the decisive point in the network that would cause the most disruption to service, in this case for over a week of virtual zero connectivity. Even though cables are being laid to supplement existing single points of failures, choke points still exist in the majority of vulnerable geopolitical areas of the world. Economic impact is severe due to prolonged outage and loss of confidence in the consumer base drives a decline in financial markets, which impacts the political system of the affected countries.

---

[195]"Repairs Begin on Middle East Web Cable," *CNN.com*, last modified February 5, 2008, http://web.archive.org/web/20080209142307/http://edition.cnn.com/2008/WORLD/africa/02/05/egypt.internet.ap/index.html (accessed March 28, 2014).

[196]Ibid.

[197]Samatha Bookman, "Submarine Cable Operators Hunt for New Routes to Counter Congestion, Political Turmoil," *Fierce Telecom*, last modified April 18, 2013, http://www.fiercetelecom.com/special-reports/submarine-cable-operators-hunt-new-routes-counter-congestion-political-turm (accessed March 28, 2014).

[198]Ibid.

The third scenario, "Resilient" describes a situation where a complex, coordinated attack is thwarted by defensive measures. Andrew Blum describes this scenario as trying to cut off New York City, where redundancy exists in the form of multiple cables and data centers.[199] Although plausible, trying to sever all the lines either in the Northeast would require time and resources that most non-state actors don't possess. The attack has the opposite effect on the target state. Societal confidence is fortified by repulse of attack but economic impact is felt in the decline in financial markets. This would describe the 2012 U.S. bank attack that was mentioned earlier where DHS and its public-private partners registered a successful repulse of non-state actors. The ability of DHS and the U.S. State Department to partner together could serve as a deterrent on future attacks by demonstrating the resolve and compency required to withstand a complex attack.

In the "Derailed" scenario, non-state actors execute a complex and coordinated attack that succeeds in creating a serious break in infrastructure. Society is initially angry with the proprietor of the attack but then that anger morphs into frustration against the local government. Economic impact is substantial as markets collapse due to lack of access by others. The attack emboldens others to attempt similar tactics. This complex attack has yet to be executed, where a physical and virtual attack combined could have catastrophic success in destroying critical infrastructure. DHS has suggested that cyber attacks on key infrastructure, the electricity system in particular, are increasing, both in frequency and sophistication.[200] The DHS research shows that the risk of a successful combined virtual and physical cyber attack, on the electric power

[199]John Brandon, "Protecting the Submarine Cables That Wire Our World," *Popular Mechanics*, last modified March 15, 2013, http://www.popularmechanics.com/technology/engineering/infrastructure/protecting-the-submarine-cables-that-wire-our-world-15220942 (accessed March 28, 2014).

[200]"National Electric Grid Remains at Significant Risk for Cyber-Attack," *Infosecurity*, last modified March 6, 2014, http://www.infosecurity-magazine.com/view/37321/national-electric-grid-remains-at-significant-risk-for-cyberattack/ (accessed April 22, 2014).

sector is "significant".[201] The disruption of essential services such as electricity would have a profound effect on the lives of the American people, and the impact would be hard to measure as almost all the remaining critical infrastructure sectors are connected to the energy sector. This type of devastating attack and the cascading effects it entails is the black swan that Nicholas Taleb describes and is the most dangerous course of action for non-state actors.

State Actor Scenarios

Figure 3. State actor scenarios

State actors represent the most dangerous threat for a cyber infrastructure attack. Andrew F. Krepinevich describes China as the most likely state actor with the capability to execute a

[201]"National Electric Grid Remains at Significant Risk for Cyber-Attack," *Infosecurity*, last modified March 6, 2014, http://www.infosecurity-magazine.com/view/37321/national-electric-grid-remains-at-significant-risk-for-cyberattack/ (accessed April 22, 2014).

cyber attack.[202] Krepinevich argues that the Chinese PLA understand American dependence on information and that "by striking directly at the 'brains, heart, and nerve centers' of the system, they can blind enemy forces.[203] Krepinevich references the ability of PLA submarines to cut undersea fiber-optic cables that provide the virtual connection between the military and the civilian economy.[204] The Chinese would utilize a combined arms approach to execute a complex attack that could isolate American forces and allow the enemy to seize the initiative. This description of a state actor will serve as the basis for following discussion.

The state actor scenarios will use the same axis as the non-state scenarios. The first scenario, Trusted Proxy, describes how proxy actors, state resourced and influenced, achieve surprise and inflict a short-term outage. Political impact is negligible, as accountability is not established but assumed. The attack doesn't warrant a political response due to the limited impact and any publicity surrounding it would only serve to lend relevancy to the rogue group or their cause. As Colin Gray describes in his book, *Another Bloody Century*, the strategic impact is negligible since the damage is not critical.[205] Social impact escalates tension between belligerents. Economic loss is limited, as recovery is responsive and timely. This scenario could describe the 2008 Middle East incident that affected Egypt and India.[206] Although the actual cause was never fully determined, and the cuts resulted in outages to a large portion of the region, access was restored in relatively short amount of time.[207] Examples of proxy actors have been documented. In February 2011, the cyber security firm McAfee Inc. announced Chinese hackers made

---

[202]Andrew F. Krepinevich, *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century* (New York: Bantam Dell, 2009), 194.

[203]Ibid, 194.

[204]Ibid., 195.

[205] Gray, *Another Bloody Century*, 324.

[206]"Repairs Begin on Middle East Web Cable."

[207]Ibid.

targeted, systematic, and long-term intrusions at five major oil and gas companies resulting in the loss of proprietary information.[208] McAfee reportedly had traced the intruder's code back to a server leasing company in Shandong Province, China.[209] This incident describes how a nation state resources a proxy actor to accomplish its military and political aims without running the risk of attribution.

The second scenario, "Shield", state actors are repelled by layered defensive measures. Although network recovery is fast, economic impact is felt by delayed recovery and realization that infrastructure is vulnerable. This situation represents a "best-case" scenario where the defender is prepared and capable of repulsing a coordinated physical and virtual attack. The Aurora test referenced earlier describes how difficult this could be for the defender. The immaturity of the majority of critical infrastructure SCADA systems highlight a vulnerability that could be easily exploited. Regardless of the limited recovery time, the fact that a complex and coordinated attack was attempted will have cascading effects in the global financial markets as confidence in network security is shaken. The biggest impact could be seen culturally as an information-driven society demands on security and access drive reform of internet security regulations. Similar to the impact the terrorist attacks of "9-11", a coordinated cyber attack could bring about the security changes that drive a cultural shift in how individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace.[210]

The third scenario, "Deep Battle", state actors are able to infiltrate infrastructure for a limited but effective attack. This type of attack is retaliatory in nature and would likely be in

---

[208]Ammilee Oliva, "China: Paper Tiger in Cyberspace" (School of Advanced Military Studies, March 29, 2012), 1, http://www.dtic.mil/dtic/tr/fulltext/u2/a566545.pdf (accessed April 22, 2014).

[209]Ibid., 2.

[210] Department of Defense, *Department of Defense: Strategy for Operating in Cyberspace*, 1.

response to sanctions or other ideological differences. In March of 2013 the South Korean financial institution attack as well as the Korean broadcaster YTN had their networks infected in an incident said to resemble past cyber efforts by North Korea.[211] The attacks came after North Korea reacted furiously after the United Nations Security Council tightened sanctions earlier that month because of its latest nuclear test.[212] The ability of North Korea to target and then effectively disable the South Korean banking system represent a decisive attack on the infrastructure that could have extended economic impacts as a prolonged outage undermines consumer confidence and halts or restricts market activity. In the case of South Korea, infrastructure resiliency is delayed by lack of regulatory oversight and governmental bureaucracy. This type of disruption could lead to escalatory attacks and lead to the next scenario.

The fourth scenario, "Force on Force", state actors execute complex and coordinated attacks that succeeds in creating a serious break in infrastructure, generating a response in kind. The 60th Anniversary of the Korean War witnessed a wave of cyber-incidents involving South Korea, North Korea, and the United States.[213] The incidents began with DDoS attacks on major South Korean websites, with corresponding retaliating attacks on North Korean government websites.[214] The US was drawn into the ongoing cyber dispute by the hacking of tens of thousands of soldiers' personal information.[215] This incident serves as an example of state on state virtual attacks, which could be combined with physical attacks to produce a catastrophic scenario where full-scale military action is taken. The conflict could escalate to where measures

[211]"A History of Cyber Attacks-a Timeline," *NATO Review*, March 2013, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, (accessed April 22, 2014).

[212]Tania Branigan, "South Korea on Alert for Cyber-Attacks after Major Network Goes down," *The Guardian*, last modified March 20, 2013, http://www.theguardian.com/world/2013/mar/20/south-korea-under-cyber-attack, (accessed April 22, 2014).

[213]Lewis, "Significant Cyber Incidents Since 2006," 16.

[214]Ibid., 16.

[215]Ibid., 16.

are enacted to fulfil Chapter VII of the United Nations charter. The impact would be substantial. World markets would grind to a halt as financial institution seal themselves off from the potential virtual attack and damaged infrastructure is repaired. Frustration against local governments build as legitimacy of the attacks are questioned, something that has already been witnessed on the Korean peninsula. Perhaps the most concerning is the success of the attack emboldens other nation states to attempt similar tactics.

Findings

The scenarios highlight parallels between both state and non-state actors. Both scenarios describe how simple attacks could be repulsed by the resiliency and redundancy of the system. The impact would be negligible as resources and technical expertise are available to mitigate network outages. This "best-case" scenario would be an attack or criminal action where there are redundant systems in place to reroute the network and public confidence in the government is high. This describes the majority of attacks that have occurred in the past, as saboteurs have only been able to execute minimal damage.

The worst case scenarios tell a different story. The opposite end of the spectrum is a complex attack, where an attack could cripple the network for an extended period of time. Both scenarios show where non-state and state actors alike could do considerable damage to the infrastructure if they know where and how to strike. Well-placed attacks that strike critical points could cause serious delays in Internet access as well shake societal confidence in the local government. This could occur in locations that are served by a limited amount of submarine cables or data centers. Africa and parts of the Middle East fit this description, where Internet

access is limited and providers have been slow to develop the network due to government regulatory stipulations.[216]

One of the secondary effects of the scenarios was societal loss of confidence in the government. When viewing the scenarios through the lens of the various driving factors show how infrastructure attacks can impact other aspects of the environment. The extent to which people believe that government can prevent cyber attacks affects whether they go about their daily lives normally and affects their tolerance for protective measures such as security measures.[217] The Internet was designed to be opened, and society is quick to respond negatively when they feel that freedom is infringed upon.[218] Public confidence in government to prevent terrorist acts also influences people's expectations that society will not experience "hard times" or worse if an attack occurs.[219] These are the indirect impacts from depressed public confidence that have a multiplier effect on the vitality of U.S. society and commerce.[220]

Recommendations

The Army Design Methodology (ADM) provides a conceptual framework that allows planners to visualize and understand the problems they face as well as the solutions necessary to

[216]Nadia Samie, "South Africa Lags Behind With Internet Access," *Voice of America*, last modified June 4, 2012, http://www.voanews.com/content/south-africa-lags-behind-with-internet-access/1147046.html (accessed March 30, 2014).

[217]T.E. Baldwin, A. Ramaprasad, and M.E. Samsa, "Understanding Public Confidence in Government to Prevent Terrorist Attack," *Journal of Homeland Security and Emergency Management* 5, no. 1 (February 2008): 3, http://www.dis.anl.gov/pubs/60939.pdf (accessed March 31, 2014).

[218]Bridget Bowman, "Internet Protest to 'fight Back' against Surveillance," *PBS Newshour*, last modified February 10, 2014, http://www.pbs.org/newshour/rundown/internet-protest-fight-back-surveillance/ (accessed March 25, 2014).

[219]Baldwin, Ramaprasad, and Samsa, "Understanding Public Confidence in Government to Prevent Terrorist Attack," 3.

[220]Ibid, 3.

bring about a desired state.[221] ADM follows a methodology of making sense of a problem, forming a theory of the phenomenon observed, creating possible ideas or solutions, and developing an operational approach to bring about the desired state. Applying this methodology to the problem of cyber infrastructure vulnerability allows the operational artist to frame the problem, which is conveyed through a narrative.

The narrative for cyber infrastructure centers on the tensions of the private-public partnership. The Internet, designed as an unsecure and open system, is in conflict with security measures that attempt to close it off from intrusive attacks. The private industry, owners of a vast majority of the infrastructure, prefer minimal regulation in an effort to keep the focus on profitability and client satisfaction. The federal government, constrained by budgetary considerations, wants to implement comprehensive and restrictive security measures without jeopardizing the private-public partnership. The government also wants to create a comprehensive authority in the Department of Homeland Security while empowering other agencies such as the Department of Defense, the National Security Agency, and the Federal Bureau of Investigations to contribute to the security plan as well. Cyber infrastructure, a relatively new entity in the global commons, is predicated upon existing telecommunications infrastructure that is unsecure and vulnerable to infiltration. Cyber infrastructure is seen as a means to delivering the western way of life to countries that for a variety of reasons reject that influence. For this reason many adversaries will view cyber infrastructure as an unwelcome intrusion to their culture. The low risk and high reward of disrupting something that represents freedom of speech and western influence offer an attraction many can't bypass.

---

[221]Department of the Army, *ADRP 5-0 The Operations Process* (Department of Defense, May 2012), 2–4, http://armypubs.army.mil/doctrine/DR_pubs/DR_a/pdf/adrp5_0.pdf (accessed February 21, 2014).

Once the narrative is constructed, a desired state can be envisioned. The desired state for cyber infrastructure is one codified authority over all aspects of the physical security that has the ability to enforce comprehensive security standards. Cyber infrastructure provides a redundant and robust structure with sensors that allow for early detection of attack and quick recovery. Private industry is regulated and adheres to security standards, which influence and serve as a basis for international norms. A strong and resilient infrastructure serves a deterrent against foreign attack, restoring societal confidence in the Internet as a secure means to conduct business.

CONCLUSION

Cyber infrastructure is vulnerable to attack, degrading Internet access. Specifically, a combined physical and virtual attack possess a significant threat to the U.S. infrastructure. The lack of documented research about the possible effects of a coordinated, complex attack reveal a planning lapse that our enemies could exploit. The absence of a coherent and inclusive cyber infrastructure defensive strategy, which has left the U.S. cyber infrastructure vulnerable to physical attack, is the result of budgetary constraints, an overreliance on private-public partnership, and a lack of a codified single authority. The private sector owns an overwhelming majority of the infrastructure and they secure it without federal oversight or adherence to federal regulations. This allows each commercial entity to interpret the security standards they deem acceptable. With most of the federal government emphasis on virtual cyberattack, risk has been accepted in the infrastructure domain in the form of the private-public partnership. The Internet as a whole is unsecure and nonstandardized, and one of the first steps to mitigating the physical risk is providing government oversight and consistent standards of security.

As this paper has shown, attacks on the cyber infrastructure can degrade access to the Internet. Although an attack is unlikely given the strategic context of the current environment, non-state actors and other rogue agents could exploit this vulnerability to great effect. DHS is the

authority in name only as other entities such as DoD have substantial roles to fulfil that DHS is not resourced for and private industry is not regulated for. DHS has begun a variety of initiatives to fulfill its responsibility for developing an integrated private-public plan for Internet recovery, but these efforts are not complete nor comprehensive.[222] Specifically, DHS has developed plans for infrastructure protection and incident response, but the components of these plans that address the cyber infrastructure are only in the beginning stages. The goal is for private industry to be held accountable to established standards that adhere to a whole-of-government approach and a defensive theory that is applicable to cyber infrastructure. Cyber infrastructure should be considered a strategic asset, and as such, DoD should be charged with physical security. This approach provides the best option as the strategic importance of CI continues to grow in the future.

[222] *Wilshusen, GAO-08-212T Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, 1.

BIBLIOGRAPHY

107th U.S. Congress. “Public Law 107-296”. U.S. Government, November 25, 2002. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed January 13, 2014).

Bajaj, Kamlesh. “The Cybersecurity Agenda: Mobilizing for International Action.” The EastWest Institute, 2010. http://www.ewi.info/sites/default/files/ideas-files/Bajaj_Web.pdf (accessed January 1, 2014).

Baldwin, T. E., A. Ramaprasad, and M. E. Samsa. “Understanding Public Confidence in Government to Prevent Terrorist Attack.” *Journal of Homeland Security and Emergency Management* 5, no. 1 (February 2008): 22. http://www.dis.anl.gov/pubs/60939.pdf. (accessed March 31, 2014).

Blum, Andrew. *Tubes: A Journey to the Center of the Internet*. New York: Ecco, 2012.

Bookman, Samatha. “Submarine Cable Operators Hunt for New Routes to Counter Congestion, Political Turmoil.” *Fierce Telecom*. http://www.fiercetelecom.com/special-reports/submarine-cable-operators-hunt-new-routes-counter-congestion-political-turm. (accessed March 28, 2014).

Bowman, Bridget. “Internet Protest to ‘fight Back’ against Surveillance.” *PBS Newshour*. http://www.pbs.org/newshour/rundown/internet-protest-fight-back-surveillance/. (accessed March 25, 2014).

Brandon, John. “Protecting the Submarine Cables That Wire Our World.” *Popular Mechanics*. http://www.popularmechanics.com/technology/engineering /infrastructure/protecting-the-submarine-cables-that-wire-our-world-15220942. (accessed March 28, 2014).

Branigan, Tania. “South Korea on Alert for Cyber-Attacks after Major Network Goes down.” *The Guardian*. http://www.theguardian.com/world/2013 /mar/20/south-korea-under-cyber-attack. (accessed April 22, 2014).

Burnett, Capt (R) Douglas R. “Cable Vision.” *Proceedings*, August 2011. http://www.usni.org/magazines/proceedings/2011-08/cable-vision (accessed February 28, 2014).

———. “Submarine Cables: Critical Infrastructure”. Squire Sanders Legal Counsel Worldwide, May 20, 2012. www.virginia.edu/colp/pdf/Burnett-Presentation.pdf (accessed February 28, 2014).

Carter, Lionel, Douglas Burnett, Stephen Drew, Graham Marle, Lonnie Hagadorn, Deborah Bartlett-McNeil, and Nigel Irvine. “Submarine Cables and the Oceans – Connecting the World.” UNEP-WCMC Biodiversity Series, 2009. http://www.iscpc.org/ publications/ICPC-UNEP_Report.pdf (accessed March 6, 2014).

Charles, Deborah. “NSA Chief Says U.S. Infrastructure Highly Vulnerable to Cyber Attack.” *Reuters*, June 13, 2013. http://www.reuters.com/article/2013/06/12/us-usa-cybersecurity-idUSBRE95B10220130612 (accessed November 1, 2013).

Cheng, Jacqui. “Phishing Plumbs New Depths: Vietnamese Fishermen Sever Fiber Optic Lines.” *Arstechnica*. Last modified June 8, 2007. http://arstechnica.com/uncategorized/2007 /06/phishing-plumbs-new-depths-vietnamese-fishermen-sever-fiber-optic-lines/ (accessed March 9, 2014).

Clarke, Richard A. *Cyber War: The next Threat to National Security and What to Do about It*. New York: Ecco, 2010.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Eliot Howard and Peter Paret, Princeton, N.J: Princeton University Press, 1976.

Clayton, Mark. “Cyberexperts: A ‘Lost Decade’ since 9/11 to Address Infrastructure Threats.” *The Christian Science Monitor*. http://www.csmonitor.com/USA/2014/0117/ Cyberexperts-a-lost-decade-since-9-11-to-address-infrastructure-threats.

CNN. “Repairs Begin on Middle East Web Cable.” *CNN.com*. Last modified February 5, 2008. http://web.archive.org/web/20080209142307/http://edition.cnn.com/2008/WORLD/africa /02/05/egypt.internet.ap/index.html (accessed March 28, 2014).

Coleman, Kevin G. “Syria and Ukraine Share Cyber Vulnerabilities.” *C4ISR & Networks*. Last modified March 3, 2014. http://www.c4isrnet.com/article/M5/20140303/C4ISRNET 18/303030009/Syria-Ukraine-share-cyber-vulnerabilities (accessed March 8, 2014).

Department of Defense. “Department of Defense: Strategy for Operating in Cyberspace”, 2011. http://www.defense.gov/news/d20110714cyber.pdf (accessed November 1, 2013).

———. “History of U.S. Missile Defense Efforts 1945-Present.” *Missile Defense Agency-U.S. DoD*. Last modified March 25, 2014. http://www.mda.mil/news/history_resources.html. (accessed March 25, 2014).

———. “Irregular Warfare: Countering Irregular Threats.” Department of Defense, May 17, 2010. http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf (accessed April 21, 2014).

———. *Quadrennial Defense Review 2014*, Department of Defense, March 4, 2014. http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (accessed March 5, 2014).

Department of Homeland Security. “2010 Communications Sector-Specific Plan”. Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf (accessed January 18, 2014).

———. “Examining the Cyber Threat to Critical Infrastructure and the American Economy.” Washington, DC: Government, March 16, 2011. http://www.gpo.gov/fdsys/pkg/ CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf (accessed March 9, 2014).

———. “Information Technology Sector-Specific Plan An Annex to the National Infrastructure Protection Plan”. Department of Homeland Security, 2010.

———. “National Infrastructure Protection Plan Fact Sheet”. Department of Homeland Security, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 18, 2014).

———. “NIPP 2013: Partnering Critical Infrastructure Security and Resilence”, 2103. http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf (accessed January 21, 2014).

———. “Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnership”. Department of Homeland Security, 2009. http://publicintelligence.net/project-12-and-the-public-private-cybersecurity-complex/ (accessed March 25, 2014).

Department of the Army. AR 525-26 Military Operations Infrastructure Risk Management. Department of the Army, June 22, 2004. http://armypubs.army.mil/epubs/525_Series_Collection_1.html (accessed March 20, 2014).

———. “Operational Environments to 2028: The Strategic Environment for Unified Land Operations”. Training and Doctrine Command, August 2012. http://www.arcic.army.mil/app_Documents/TRADOC_Paper_Operational-Environments-to-2028-Strategic-Environment-for-Unified-Land-Operations_AUG2012.pdf (accessed March 28, 2014).

Farwell, James P. “Industry’s Vital Role in National Cyber Security.” *Strategic Studies Quarterly* (Winter 2012): 32.

Fox News. “Target, Neiman Marcus Executives Apologize for Data Breach.” *Fox News*. http://www.foxnews.com/politics/2014/02/05/target-neiman-marcus-executives-apologize-for-data-breach/ (accessed February 6, 2014).

Freedman, Lawrence. *Deterrence*. Cambridge, UK: Malden, MA: Polity Press, 2004.

Fryer-Biggs, Zachary. “US Cyber Moves Beyond Protection.” *Defense News*. Last modified March 16, 2014. http://www.defensenews.com/article/20140316/DEFREG02/303170013/US-Cyber-Moves-Beyond-Protection (accessed March 20, 2014).

Geary, James. “Who Protects the Internet?,” March 13, 2009. http://www.popsci.com/scitech/article/2009-03/who-protects-intrnet?nopaging=1. (accessed November 1, 2013).

Gertz, Bill. “Chinese Military Is Targeting Critical U.S. Infrastructure for Cyber Attacks, Report Says.” *Flash//CRITIC Cyber Threat News*. http://flashcritic.com/chinese-military-is-targeting-critical-u-s-infrastructure-for-cyber-attacks-report-says/ (accessed March 24, 2014).

Goss, Thomas. "'Who's in Charge?' New Challenges in Homeland Defense and Homeland Security." *Homeland Security Affairs*, no. 2 (2006): 14. http://www.hsaj.org/?fullarticle=2.1.2 (accessed March 28, 2014).

Gray, Colin S. *Another Bloody Century: Future Warfare*. London: Phoenix, 2006.

Gray, Colin S, Army War College (U.S.), and Strategic Studies Institute. *Making Strategic Sense of Cyber Power Why the Sky Is Not Falling*. Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2013. http://purl.fdlp.gov/GPO/gpo36745. (accessed November 6, 2013).

Green, Mick, Stephen Drew, Lionel Carter, and Douglas Burnett. "Submarine Network Security." International Cable Protection Committee, April 13, 2009.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations." *The Guardian*. Hong Kong, June 9, 2013. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed January 18, 2014).

Headquarters, Department of the Army. "FM 3-38 Cyber Electromagnetic Activities". Headquarters, Department of the Army, February 2014. http://armypubs.army.mil /doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf (accessed February 28, 2014).

Huth, Paul, and Bruce Russett. "What Makes Deterrence Work? Cases from 1900 to 1980." *World Politics* 36, no. 4 (July 1984): 32. http://www.jstor.org/stable/2010184 (accessed April 21, 2014).

Infosecurity. "National Electric Grid Remains at Significant Risk for Cyber-Attack." *Infosecurity*. Last modified March 6, 2014. http://www.infosecuritymagazine.com/view/37321/ national-electric-grid-remains-at-significant-risk-for-cyberattack/ (accessed April 22, 2014).

ISCPC. "About Submarine Telecommunications Cables". International Cable Protection Committee, October 2011. http://www.iscpc.org/publications/About_SubTel_Cables_2011.pdf (accessed March 8, 2014).

Jensen, Eric Talbot. "Cyber Deterence." *Emory International Law Review* 26 (2012): 52. http://www.law.emory.edu/fileadmin/journals/eilr/26/26.2/Jensen.pdf (accessed February 28, 2014).

Johnson, Keith. "GOP Scuttles Law-of-Sea Treaty." *The Wall Street Journal*, July 16, 2012. http://blogs.wsj.com/washwire/2012/07/16/gop-opposition-scuttles-law-of-sea-treaty/ (accessed March 14, 2014).

Krencik, Jim. "Telecom Reps Offer Testimony at Rural Broadband Hearing." *The Daily News*, March 21, 2014. http://thedailynewsonline.com /news/article_4c6ab52e-b0ac-11e3-baa4-001a4bcf887a.html (accessed March 25, 2014).

Krepinevich, Andrew F. *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century*. New York: Bantam Dell, 2009.

Langevin, James, Michael McCaul, Scott Charney, Harry Raduege, and James Lewis. "Securing Cyberspace for the 44th Presidency." Center for Strategic and International Studies, n.d. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed January 1, 2014).

Leppard, David. "Al-Queda Plot to Bring Down UK Internet." *Martinfrost*, March 11, 2007. http://www.martinfrost.ws/htmlfiles/mar2007/aqweb_plot.html (accessed November 1, 2013).

Lewis, James. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." Center for Strategic and International Studies, 2002.

———. "Significant Cyber Incidents Since 2006". Center for Strategic and International Studies, October 10, 2013. http://csis.org/files/publication/131010_Significant_Cyber _Incidents_Since_2006%20(3).pdf.

Libicki, Martin C. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly* 8, no. 1 (Spring 2014). http://www.au.af.mil/au/ssq (accessed March 14, 2014).

Libicki, Martin C., and Project Air Force (U.S.). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

Mack, Eric. "Google Outage Reportedly Caused Big Drop in Global Traffic." *CNET*. http://www.cnet.com/news/google-outage-reportedly-caused-big-drop-in-global-traffic/. (accessed Marh 28, 2014).

Magnuson, Stew. "Feds Fear Coordinated Physical, Cyber-Attacks on Electrical Grids." *National Defense*, September 2012. http://www.nationaldefensemagazine.org/archive/2012/ september/Pages/FedsFearCoordinatedPhysical,Cyber-AttacksonElectricalGrids.aspx. (accessed April 24, 2014)

Martin, Jr., James. "Paradigm Change: Cybersecurity of Critical Infrastructure". Joint Advanced Warfighting School, Norfolk, VA: Joint Forces Staff College, 2013.

Matis, Michael. "The Protection of Undersea Cables: A Global Security Threat". Carlisle Barracks, PA: U.S. Army War College, 2012.

Mearsheimer, John. "Back to the Future." *International Security* 15, no. 1 (Summer 1990): 52. http://www.jstor.org/stable/2538981 (accessed March 28, 2014).

Miller, Jason. "DHS Revs up Its Part of the Cyber Executive Order." *Federal News Radio*. Last modified January 31, 2014. http://www.federalnewsradio.com/?nid=473&sid=3553526 &pid=0&page=1 (accessed February 6, 2014).

Nakashima, Ellen. “Obama Signs Secret Directive to Help Thwart Cyberattacks.” *The Washington Post*. http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html (accessed February 6, 2014).

———. “U.S. Rallied 120 Nations in Response to 2012 Cyberattack on American Banks.” *Washington Post*, April 11, 2014. http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html (accessed April 22, 2014).

National Research Council (U.S.), and National Academies Press (U.S.). *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. Edited by John L. Hennessy, David A. Patterson, and Herbert Lin. Washington, D.C: National Academies Press, 2003.

NATO. “A History of Cyber Attacks-a Timeline.” *NATO Review*, March 2013. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (accessed April 22, 2014).

Odierno, GEN Raymond. “CSA Strategic Priorities”. Department of the Army, October 13, 2013. http://usarmy.vo.llnwd.net/e2/c/downloads/316390.pdf (accessed March 6, 2014).

Oliva, Ammilee. “China: Paper Tiger in Cyberspace”. School of Advanced Military Studies, March 29, 2012. http://www.dtic.mil/dtic/tr/fulltext/u2/a566545.pdf (accessed April 22, 2014).

Pilot, Fred. “http://eldotelecom.blogspot.com/2014/03/us-at-Inflection-Point-on-Premises.html.” *Eldo Telecom*, March 22, 2014. http://eldotelecom.blogspot.com/2014/03/us-at-inflection-point-on-premises.html (accessed March 25, 2014).

President George W. Bush. The National Security Strategy of the United States of America. The White House, September 17, 2002. http://georgewbushwhitehouse.archives.gov /nsc/nss/2002/ (accessed April 21, 2014).

Rappaport, Jocelyn. *On the Map: As Controversy Swirled around His Dissertation, Sean Gorman Realized His Future and Founded a Company*, 2004. http://spirit.gmu.edu/archives /winter08/on_the_map.html (accessed November 1, 2013).

Samie, Nadia. “South Africa Lags Behind With Internet Access.” *Voice of America*. Last modified June 4, 2012. http://www.voanews.com/content/south-africa-lags-behind-with-internet-access/1147046.html (accessed March 30, 2014).

Sasso, Brendan. “After Defeat of Senate Cybersecurity Bill, Obama Weighs Executive-Order Option.” *The Hill*. Last modified August 4, 2012. http://thehill.com/blogs/hillicon-valley/technology/242227-with-defeat-of-cybersecurity-bill-obama-weighs-executive-order-option (accessed February 6, 2014).

Schwartz, Peter. *The Art of the Long View*. 1st ed. New York: Doubleday/Currency, 1991.

Sechrist, Michael. "CYBERSPACE IN DEEP WATER: PROTECTING UNDERSEA COMMUNICATION CABLES By Creating an International Public-Private Partnership". Harvard Kennedy School, March 23, 2010. http://belfercenter.hks.harvard.edu /files/PAE_final_draft_-_043010.pdf. Accessed March 9, 2014.

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

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. 2nd ed., Random trade pbk. ed. New York: Random House Trade Paperbacks, 2010.

The White House. "Cyber Security." *The White House*. Last modified Unknown.. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity (accessed January 18, 2014).

———. "Presidential Decision Directives - PDD 63." Government. *Presidential Decision Directives - PDD*. Last modified May 22, 1998. https://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed March 1, 2014).

———. "Presidential Policy Directive 21". The White House, February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed January 12, 2014).

Timberg, Craig. "NSA Slides Explain the PRISM Data-Collection Program." *Washington Post*, July 10, 2013. http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (accessed November 1, 2013).

Timberg, Craig, and Ellen Nakashima. "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance." *Washington Post*, July 10, 2013.. http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html (accessed March 24, 2014).

Troianovski, Anton. "Optical Delusion? Fiber Booms Again, Despite Bust." *The Wall Street Journal*, April 3, 2012. http://online.wsj.com/news/articles/SB10001424052702303863404577285260615058538 (accessed March 8, 2014).

U.S. Army War College. *Cyber Infrastructure Protection*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011.

United States. *Cybersecurity and Homeland Security*. New York: Nova Science Publishers, Inc, 2005.

United States Army. "ADRP 5-0 The Operations Process". Department of Defense, May 2012. http://armypubs.army.mil/doctrine/DR_pubs/DR_a/pdf/adrp5_0.pdf (accessed February 21, 2014).

Washburn, Frank. “Will Internet Sabotage Hit Home?” *PC Magazine,* June 1, 2008. http://www.pcmag.com/article2/0,2817,2316780,00.asp (accessed November 1, 2013).

White House. “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure”. White House, 2009. http://www.whitehouse.gov/assets /documents/Cyberspace_Policy_Review_final.pdf (accessed December 30, 2013).

Wilkinson, Lawrence. “How to Build Scenarios Planning for ‘long Fuse, Big Bang’ Problems in an Era of Uncertainty.” *Wired*, 1995. http://www.wired.com/wired/scenarios/build.html. (accessed March 26, 2014).

Wilshusen, Gregory. “GAO-08-212T Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan”. United States Government Accountability Office, 2007. http://www.gao.gov/products/GAO-08-212T (accessed October 12, 2013).

Cyberpower and National Security. 1st ed. Washington, D.C: National Defense University Press : Potomac Books, 2009.

“National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency”. Department of Homeland Security, 2009. http://www.dhs.gov/xlibrary/assets/ NIPP_Plan.pdf (accessed January 6, 2013).

Roots of Strategy. Mechanicsburgh, PA: Stackpole Books, 1987.

“Senators Portman and Ayotte Sink Law Of The Sea Treaty.” *Rob Portman, United States Senator for Ohio*. Last modified July 16, 2012. http://www.portman.senate.gov /public/index.cfm/press-releases?ID=a886f01e-1b08-4c51-bf7e-4bad33194c0b (accessed March 6, 2014).