The Securitization of Cyberspace through Technification

Kevin J. Schwarz

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Arts
In
Political Science

Priya Dixit, Committee Chair
Scott G. Nelson
Paul C. Avey

April 28, 2016
Blacksburg, VA

Keywords: Political Science

The Securitization of Cyberspace through Technification

Kevin J. Schwarz

ABSTRACT

This thesis adds to the literature surrounding technification in securitizing cyberspace by examining the role of technical experts in constituting threats in cyberspace at the level of the state. Furthermore, this thesis considers the impact of technocratic framing on the public's understanding of cyberspace and the historical conditions under which this framing developed.

Table of Contents

Introduction **1**
Literature Review 5
Chapter 1 ..... **12**
Eligible Receiver 13
Risk and Future Threats 17
Experts' Framing of Cyberspace 21
Cyberspace Technified and Tied to Experts for Understanding 28
Chapter 2 ..... **31**
The Patriot Act 33
Expert Organizations 35
Chapter 3 ..... **46**
Characterizing Cyberspace as a Threat 48
Characterizing Cyberspace as Vulnerable to Threats 55
Technification 59
Conclusion **68**
Acknowledgements **72**
Bibliography **73**

Introduction

Across the globe "participation in cyberspace is growing at a remarkably rapid rate,"[1] creating a new realm for global communication and interaction. Cyberpolitics has shifted from low politics, related to routine decisions and processes, to high politics concerning decision systems critical to the state, core institutions, and national security.[2] As the stakes of cyberpolitics have increased, states have attempted to manage cyberspace and policy, especially in their efforts to secure it from perceived threats. In the United States, institutions such the Department of Homeland Security have been established partly to secure cyberspace against emerging threats. There has also been the formation and establishment of US Cyber Command. The broad question this thesis explores is how have threats to national security been conceptualized as taking shape in cyberspace? This thesis argues that the United States has securitized cyberspace through technification, understood as "constitution of an issue as reliant upon expert, technical knowledge for its resolution."[3] Technification facilitates political acceptance amongst the population while elevating the status of experts and giving them significant decision-making power. Thus, technification gives technology experts epistemic authority to constitute threats in cyberspace.

Cyber security experts are a select few, whose technical expertise takes years of study to master. These experts use their knowledge for a variety of purposes, including creating applications, diagnosing problems, and educating users. As the field of cyber

---

[1] Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, Mass.: MIT Press, 2012, 66.
[2] Ibid., 3.
[3] Hansen, Lene, and Helen Nissenbaum. 2009. Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly* 53 (4): 1157.

security within computer science has developed, these experts have used analogies, similes, and metaphors to make the discourse of computer networks and systems available to the public. Terms like viruses, worms, and firewall allow cyber security experts to convey technical concepts in a simplified and intuitive manner to non-technical users drawing on cultural resources. Non-IT people can understand the security implications of these threats. A virus infects its host while a worm hides itself deep within the system and the firewall provides a line of defense. Discourse plays a critical role in framing cyber security concepts for the public to grasp the political significance of technology and threats. Yet, the rapid pace of technological development means much information is not readily available to the general public, but is instead reserved for experts.[4] As a result, technocratic cyber security experts are given a kind of epistemic authority and legitimacy in the practice of constituting the domain of cyber security, especially the attendant threats. For instance, in the United States after September 11th, the Office of Homeland Security (later the Dept. of Homeland Security) was established and given the role to specialize as 'lead agency' in the protection of IT.[5] This thesis will examine the role of these types of organizations in constituting security threats in cyberspace.

The authority of technocrats in this area is rarely questioned because technocrats are treated as extensions of technology. The assumption is that technocrats "construct an issue as reliant upon technical, expert knowledge, but they also simultaneously

---

[4] Nissenbaum, H. 2005. Where Computer Security Meets National Security. *Ethics and Information Technology* 7 (2). 72.
[5] US Dept. of Homeland Security. 2003. "The National Strategy to Secure Cyberspace" 16.

presuppose a politically and normatively neutral agenda that technology serves."[6] Consequentially, technocrats are treated as offering unbiased knowledge and trusted to frame cyber security issues in a manner that is objective and neutral. But framing is not a neutral practice. According to Judith Butler, framing is the power to "selectively produce[s] and enforce[s] what will count as reality."[7] Cyber realities are experienced and understood by the population by virtue of their frame. By controlling the content of reality in cyberspace, cyber security technocrats have the power to shape a reality. This reality is often accepted as natural, given, and necessary instead of as a product of contingent decisions about what aspects to prioritize as a threat or risk when the possible versus the probable is unknown. However, these realities, which are socially constructed, can become useful for state agendas. Framing something in a specific way, like cyberspace as technical, can remove other concerns, such as ethical or political, from the discussion. Furthermore, this can be used to get the population to support exceptional measures taken in the name of security.

Technocratic framing is especially important in the context of cyber threats because it informs people's decisions or desires when it comes to taking actions that involve violence. By framing cyber attacks as exceptional threats to national security, exceptional responses can be justified. In 2011, the White House stated it would "respond to hostile acts in cyberspace as we would to any other threat to our country [and reserved]

---

[6] Hansen, Lene, and Helen Nissenbaum. 2009. Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly* 53 (4)., 1167.
[7] Butler, Judith. 2009. *Frames of War: When Is Life Grievable?* London: Verso, 2009. Xiii.

the right to use all necessary means"[8] including military action. In August 2015, the United States made good on its threat by carrying out a drone strike in Syria, killing Junaid Hussain. Hussain allegedly aided in the hack of CENTCOM's twitter account and website, and released the personal information of US military personnel on behalf of ISIS.[9] US officials thus demonstrated their willingness to respond to cyber threats with military action, meaning the cyber threats were deemed exceptional enough to warrant the exceptional response of violence.

This thesis will therefore offer a consideration of who frames the threats in cyberspace and the implications of this framing on claims of exceptional authority. Through the framing by technocrats, the public can understand the threats in cyberspace. However, technification often depoliticizes debates with language that makes the debate inaccessible to non-specialists while giving the specialist or expert considerable decision-making power. Recognizing the role of technology in the mitigation of risk society, as well as the contentions that create insecurity in cyberspace, this thesis will explore the role of experts in constituting security and insecurity in cyberspace. This thesis will argue that cyberspace, and security within it, has been conceptualized as technical in nature. In turn, cyber security has undergone technification, where it is entrusted only to specialists. After 9/11, cyberspace was securitized against exceptional threats posed to critical infrastructure. The securitization is maintained through the process of technification, under which cyber security is deemed "so critical it should not be left to amateurs."[10]

---

[8] White House. 2011. *INTERNATIONAL STRATEGY FOR CYBERSPACE Prosperity, Security, And Openness In A Networked World*.
[9] Lawson, Sean. "With Drone Strike On ISIS Hacker U.S. Escalates Its Response To Cyber Attacks" Sept 12, 2015. Forbes
[10] Hansen and Nissenbaum, 1167

This thesis will examine the technification of cyber security during the Clinton administration and then examine how technocrats constitute threats in cyberspace on behalf of the American people during that period and afterwards.

First, a literature review will be provided to outline current arguments and debates in the field relevant to this thesis. The first chapter will focus on the late 1990s during the Clinton Presidency. This chapter will examine *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*, a report published by the Clinton administration assessing cyber vulnerabilities in critical infrastructures. The report presents cyberspace as a potential risk to national security that is uniquely is technical and complex. The following chapter will examine the time period in the aftermath of September 11th during the George W. Bush Presidency. President Bush created a number of organizations to protect the US from terrorist threat, many of which acted to secure cyberspace. Additionally, the chapter will examine the process through which a national strategy was formed to secure cyberspace from threats. The final chapter will examine the *The National Strategy to Secure Cyberspace* and how it securitizes cyberspace by presenting it as technical. The thesis will conclude by considering the impact technification, and how it securitizes cyberspace while giving technical experts the ability to frame threats in that space.

Literature Review

This literature review will outline concepts that will be used for analysis in the thesis. First I will review the literature surrounding risk society, specifically in the context of technology and future uncertainty since the literature surrounding risk society and cyber security is sparse. After outlining the literature in risk society, I will provide an

overview of the Copenhagen School's Securitization Theory. Finally, I will review literature in international relations surrounding technification, within the context of cyber.

Central to the development of cyberspace has been the application of technical knowledge. Choucri notes that in the digital age, "cyber access becomes both a cause and a consequence of the global race for knowledge and thus points to the power underpinnings of world politics and the competitive edge in the world economy."[11] Cyber venues have led to a transition to a knowledge-based economic system where knowledge paired with information technology is a driving force for power. Simultaneously, as both a cause and effect of the global race for knowledge, cyber access acts as a culturally and economically globalizing force by providing a venue for political interaction. However, a new global digital age comes with its own set of dangers.

Within cyberspace there are a number of debates about its role in future conflict. Many people in defense circles, like former White House 'cyber czar' Richard Clarke, have argued that cyber attacks will be amongst the greatest dangers to national security in the twenty-first century as more systems become 'connected' and vulnerable. Officials like former Director of National Intelligence Mike McConnell and former Defense Secretary/Director of the CIA Leon Panetta have voiced similar concerns about the threat of cyber attacks to national security and its impact on warfare. Some scholars in International Relations have sided with these officials. Similar to Clarke, Gary McGraw believes that cyber war is "inevitable unless we improve our cyber defenses"[12] for critical infrastructures that are vulnerable to attack. John Stone of the Department of War Studies

---

[11] Choucri, 71.
[12] Mcgraw, Gary. "Cyber War Is Inevitable (Unless We Build Security In)."*Journal of Strategic Studies* 36, no. 1 (2013): 109-19.

at King's College believes that cyber attacks could be construed as acts of war since these attacks can utilize force that is violent and even potentially lethal.[13]

Other scholars in international relations believe that the fear of 'cyber war' may be exaggerated. For example, Lindsay credits widespread concern of a 'cyber revolution' in conflict to faulty assumptions about conflict in cyberspace. Linsday writes that it is widely believed that "cyberwarfare is asymmetric, that the offense has the upper hand, and deterrence models of assured retaliation do not apply to cyberspace [since] it is difficult and time consuming to identify an attack's perpetrator"[14] due to the attribution problem. However, Lindsay argues that cyber weapons are certainly not weapons of the weak providing small groups or countries asymmetric advantages because the resources required to conduct a sophisticated cyber attack are unavailable to most nations. Thus, "there are operational barriers to entry for strategic cyber warfare that discourage weak actors from attempting."[15] Regardless of sophistication, cyber attacks carry nonzero probabilities that they will be compromised, be attributed, or fail.[16] Similarly, as intensity of attack increases, the chance of remaining anonymous decreases, and consequentially the likelihood of retaliation increases. The threat of retaliation acts as a defense that "make[s] offensive aggression unwise."[17] As a result, Lindsay dismisses the common assumptions used to build the 'cyber revolution' and the newest emerging threat in warfare. Thomas Rid also does not believe there will be a 'cyber revolution' in conflict that will create the possibility of cyber wars. In fact, Rid argues that cyber attacks are not

---

[13] Stone, John. 2013. Cyber war will take place. *The Journal of Strategic Studies*36 (1): 101-8.
[14] Lindsay, JR. 2013. Stuxnet and the limits of cyber warfare. *Security Studies* 22 (3): 374
[15] Ibid., 397.
[16] Ibid., 388.
[17] Ibid., 395

really very new, they are merely more sophisticated versions of three tactics that have been around for ages: sabotage, espionage, and subversion.[18] Thus, the role of cyber weapons and 'cyber war' in future conflict is debated within the field of international relations. Scholars like John Mueller, Peter Singer, and Noah Shachtman make similar arguments to Rid suggesting that the threat of cyber war may be overstated.

While technological advancements aid in the development and improve of knowledge and society, they also create new risks. Similarly, although scholars debate how sizable an impact cyberspace will make on conflict, both sides ultimately recognize that cyberspace creates new risks. Ulrich Beck notes that most risks to security in late modernity[19] are man-made manufactured risks which have resulted in the development of a risk society, understood as "a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself."[20] Thus, modernization has created the risks that threaten humanity such as pollution, nuclear radiation, etc. While Beck's analysis of risk society is framed in terms of ecological consequences, Anthony Giddens expands upon the literature regarding Beck's concept of risk society specifically in terms of technology. Giddens argues "a risk society is a society where we increasingly live on a high technological frontier which no one really understands, and which generates a diversity of possible futures."[21] Rapid growth in knowledge and advancements made in information technology become truly unfathomable. Moore's Law has shown that computer-based technologies are exponential in their growth. Given the uncertainty that

---

[18] Rid, xiv.
[19] Which Beck refers to as reflective modernity because it opposes the first modernity by undoing many of its institutions such as the welfare state, political parties, etc.
[20] Beck, Ulrich (1992) *Risk Society: Towards a New Modernity*. London: Sage., 21.
[21] Giddens, Anthony. 1999. "Risk and Responsibility". *The Modern Law Review* 62 (1). Wiley., 3.

stems from a diversity of possible futures, risk societies are "increasingly preoccupied with the future (and also with safety), which generates the notion of risk."[22] Thus, risk societies arise from the uncertainty of the future driven by technological advancement that characterizes the digital age. This thesis will look to the concept of risk society as a reason for the emergence of technical experts in cyber security. Experts were trusted to mitigate risks and vulnerabilities in critical infrastructure resulting from technological advancement, including fears of catastrophic attacks capable of disabling whole defense systems and power grids.

Risk society, and focus on managing risk in the face of an increasingly technologically advanced yet uncertain future, is tied closely to determining what counts as an issue of security. International relations and security studies scholars alike have studied the process of how issues become framed in terms of security, specifically through studies of securitization. Securitization theory has its origins in the Copenhagen School with scholars such as Barry Buzan, Ole Wæver and Jaap de Wilde. The Copenhagen School argues security is a speech act. Buzan et al. write that securitization moves referent objects from matters of regular politics to matters of security that warrant exceptional urgency by using speech acts that persuade an audience to accept the issue as a security threat.[23] Securitizing agents usually hold power[24] and influence over audiences.

---

[22] Ibid., 3.
[23] Buzan, Barry, and Ole Ver. *Security: A New Framework for Analysis*. Boulder, Colo.: Lynne Rienner Pub., 1998., 23.
[24] I adopt a comprehensive definition of power from Morgenthau, who writes that power "may comprise anything that establishes and maintains the control of man…power covers all social relationships which serve that end, from physical violence to the most subtle psychological ties by which one mind controls another"
Morgenthau, Hans J., and Kenneth W. Thompson. 1985. *Politics among nations: The struggle for power and peace*. 6th ed. New York: McGraw-Hill., 11.

Securitization occurs at different levels (local, regional, non-regional/subsystemic, and global) and is analyzed across sectors (military, economic, environmental, political, and societal)[25] that act as referent objects to be compared and contrasted. Cyberspace complicates securitization theory ontologically since it simultaneously acts as a level at which events occur and as a sector that acts as a referent object. Within the Security Studies discipline, a handful of scholars have examined the implications of cyberspace on securitization theory.

Hansen and Nissenbaum use the Copenhagen School as guidance to argue the "political importance [of cyber-related referent objects] arises from connections to the collective referent objects of 'the state,' 'society,' 'the nation,' and 'the economy.'"[26] Furthermore, they argue that cyber referent objects are threatened through three forms of securitization:

> hypersecuritization, which identifies large-scale instantaneous cascading disaster scenarios; everyday security practices, that draws upon and securitizes the lived experiences a citizenry may have; and technifications, that captures the constitution of an issue as reliant upon expert, technical knowledge for its resolution and hence as politically neutral or unquestionably normatively desirable.[27]

Others have used these forms of securitization in the discipline. Hjalmarsson argues that Hansen and Nissenbaum's concept of hypersecuritization is used by the US Government to securitize cyberspace under the Obama administration. US officials present cyberspace as "a series of connected referent objects, bound together by a network [that is] presented

---

[25] Kremer, Jan, and Benedikt Müller, eds. *Cyberspace and International Relations: Theory, Prospects and Challenges*. Springer, 2014., 66
[26] Hansen, Lene, and Helen Nissenbaum. 2009. Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53 (4).,1155
[27] Ibid., 1157.

as under constant threat of attack by omnipresent adversaries."[28] Hansen and Nissenbaum's final form of securitization, technification, was of particular interest to this project. Norman Girvan examines the concept of technification broadly in his analysis of Economic Partnership Agreements between Caribbean countries and the European Union. He contends that technification is the "use of technical jargon in policy debates in ways that restrict broad political participation in decision-making."[29] In his study, he finds that technification is used to exaggerate or obscure the benefits of the agreement in order to facilitate political acceptance while simultaneously elevating the status of the few with trade expertise. While Hansen and Nissenbaum make a similar argument that technification is used to facilitate political acceptance (of a cyber security threat), cyber security experts "construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves."[30] Experts are given epistemic authority over a cyber domain that is constructed as technical and therefore unavailable to the politicians or the public. Consequentially, they act as securitizing actors while still distinguishing themselves from political actors because their knowledge is treated as neutral.

This thesis seeks to add to the literature surrounding technification in securitizing cyberspace by examining the role of technical experts in constituting threats in cyberspace at the level of the state. Furthermore, this thesis will consider the impact of technocratic framing on the public's understanding of cyberspace and the historical conditions under which this framing developed.

---

[28] Hjalmarsson, Ola. "How the Web Was Won." Master's thesis, Lund University, 2013.
[29] Girvan, Norman. 2010. technification, sweetification, treatyfication. *Interventions* 12 (1)., 100.
[30] Hansen and Nissenbaum, 1167

Chapter 1

By the second term of the Clinton Administration (1997-2001), the dot-com boom was well under way. At the click of a button, resources from around the world were rapidly being made available to people using the World Wide Web. While cyberspace connected the world and offered new venues for exchange, interconnectivity also created vulnerabilities to critical infrastructure that were increasingly connected. The Clinton Administration encouraged larger roles for experts and industry leaders through collaborative public-private partnerships in managing future risks and vulnerabilities in critical infrastructure. In order to convey vulnerabilities that were perceived as complex or technical, the Administration relied heavily on assessing future implications cyberspace could have on collective referent objects;[31] like the national security, the state, and economy through the development of critical infrastructure. In other words, threats were presented as future looking, which limited the securitization of cyberspace since the threats were not immediate. Furthermore, this practice helped engrain the role of technical experts as the people who could tie the technical components that make up cyberspace to collective referent objects. Instead of using foreign policy or national security analysts' assessments, computer scientists and IT personnel would be used to articulate what "cyber issues" and especially "cyber threats" were. As a result, cyberspace was technified, or reliant on technical experts for understanding.

After providing more historical context, this chapter will analyze "The Report of the President's Commission on Critical Infrastructure" from October 1997 and related developments surrounding it. This analysis demonstrates the preoccupation with the

[31] Similar to those noted in: Hansen and Nissenbaum, 1155

future along with reliance on experts to connect technical vulnerabilities to collective referent objects. Finally, the chapter will conclude by arguing that while the *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure* helped to connect cyberspace to national security through critical infrastructure, it did not securitize cyberspace. Rather, the report conceptualized cyberspace in terms of risk, which could be managed by technical experts. As yet, cyberspace was not a direct threat to national security, but rather a future threat still on the horizon.

Eligible Receiver

The impact of the computer age on national security was familiar to the American public. Hollywood science fiction movies like *WarGames (1983)* introduced the American public to the idea of a new and fast approaching modern world where hackers could use backdoors to gain access to critical defense systems, like NORAD, and bring the world to the brink of war. In summer of 1997, a no notice Joint Chiefs of Staff military exercise named Eligible Receiver gave the US Government one of its first big cyber scares, demonstrating that dangers in cyberspace were no longer science fiction but reality. Eligible Receiver sought to test "DoD planning and crisis action capabilities when faced with attacks on DoD information infrastructures."[32] Unaware that the attacks were part of an exercise, military commands and government agencies would react to attacks as if the situation were real. Eligible Receiver would give the Joint Chief direct insight to DoD readiness for a large-scale cyber attack.

[32] Pike, John. "Military: Eligible Receiver." Global Security. May 7, 2011. Accessed February 18, 2016. http://www.globalsecurity.org/military/ops/eligible-receiver.htm.

Eligible Receiver took on two phases, both carried out by a Red Team[33] of computer experts from the NSA "with no inside information."[34] Cyber tools were first used to attack energy and telecommunication infrastructure that was both publicly and privately held. Concurrently, the Red Team leveraged open source information readily available on the Internet to penetrate DoD networks. While much of the information about the results of the exercise remains classified, it is clear that both phases of the attacks were successful in their mission. The NSA Red Team achieved "unprecedented victories;"[35] successfully penetrating a number of government networks, denying service, and in some cases even gaining systems administrator/super-user level privileges that would allow them to add/remove users and reformat server hard drives. They also reportedly had the capability to control power grids and 911 in nine US cities.[36] Had these attacks been real and not a military exercise, attackers had sufficient access and control over networks to disrupt and degrade US military bases' "ability to deploy and sustain forces."[37] Consequentially, Eligible Receiver served as a wake up call for the US military demonstrating ill preparedness for potential cyber threats. Cyber threats to national security were no longer merely a science fiction fantasy dreamed up by

---

[33] A Red Team is an independent group used in exercises and war games to challenge an organization, usually acting as the adversary

[34] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., 8

[35] Magnan, Stephen W. "Safeguarding Information Operations: Are We Our Own Worst Enemy." Central Intelligence Agency. June 27, 2008.

[36] PBS. "Cyberwar: Warnings." PBS. April 4, 2003.

[37] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., 8.

Hollywood directors, but also an increasingly new and challenging reality keeping Pentagon officials awake at night.

Cyberspace and the cyber threats that come along with it presented a new element of danger to the United States. The same technical sophistication that had fueled arms and space races against the Soviet Union was beginning to make United States vulnerable to new types of threats. During the 1990s, there was widespread belief within US policy circles that "the day may be coming where an enemy can attack [the US] from a distance, using cyber tools, without first confronting our military power and with a good chance of going undetected."[38] Eligible Receiver served as a prime example that these future fears could be realized much sooner than expected. With great uncertainty surrounding this new 'cyber' venue, specifically with its effects on critical infrastructure, President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP).[39]

The PCCIP was comprised of specialists from most major executive branch departments and agencies along with representatives from private industry and academia.[40] The Commission was established to address physical and cyber threats to critical infrastructure, defined as "physical threats to tangible property and threats of electronic, radio-frequency, or computer-based attacks on the information or

---

[38] Ibid., 8.
[39] The President's Commission on Critical Infrastructure Protection will be referred to as the 'PCCIP' or the 'Commission' interchangeably throughout this paper
[40] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., iii-iv

communications components that control critical infrastructures,"[41] respectively. This team of experts would compile a full assessment of potential vulnerabilities and threats to critical infrastructures then recommend national policy as well as an implementation strategy to assure continued operation. The Commission, chaired by Gen. Robert Marsh, released their report in October 1997 addressing vulnerabilities created by increasing dependence on ICT in infrastructure as well as ways these vulnerabilities could be managed.[42] [43]

The report's understanding of the challenges in cyberspace shares many characteristics with risk society. Risk society is the development of "a systematic way of dealing with the hazards and insecurities introduced by modernization itself."[44] Risk society is similar to securitization in its focus on existential threats. Furthermore, both are dealt with through technification, where technical expertise is used to mitigate or respond to risks and threats. Cyber threats to critical infrastructure were a direct result of the advancements made in information communication technology that allowed for the development of the Internet and the emergence of cyberspace as a factor in national security. Ulrich Beck argues that as the capacity of technical option grows, so does the incalculability of their consequences.[45] In critical infrastructure, the PCCIP remarked that the complexity made it so that "it may be impossible to determine the nature of a threat

---

[41] Executive Order 13010 of July 15, 1996, Critical Infrastructure Protection. Code of Federal Regulations, (1996): 37347.
[42] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., I
[43] Executive Order 13010 of July 15, 1996, Critical Infrastructure Protection. Code of Federal Regulations, (1996): 37347 -37350
[44] Beck, 21
[45] Beck, 22

until after it has materialized."[46] Thus, technical complexities of interconnected systems where vulnerabilities can cascade make risks unknowable until after an attack occurs. The PCCIP report demonstrated characteristics of risk society through its focus on the future, its characterizations of security risk as a result of cyberspace, and finally its dependence on technical experts to construct the risk discourses that act as the basis for policy agendas.

Risk and Future Threats

Within risk society, technology is a potential cause of risk, but also increasingly a means through which future risks can be managed. Giddens writes that in risk society, "we increasingly live on a high technological frontier which absolutely no one completely understands and which generates a diversity of possible futures."[47] Uncertainty leads to framing the future in terms of risk, which in turn generates anxiety due to the uncertainty, which results in higher perception of risk. Uncertainty, therefore, creates risk, which threatens the perception and feeling of safety and security. Consequentially, much focus is devoted to understanding possible futures so that they may be managed in the name of security. The narrative of the PCCIP's report fits this mold as it was very preoccupied with the future and sought to address vulnerabilities in critical infrastructure primarily to secure against 'new' (cyber) threats.

The primary mission of the PCCIP per its founding executive order was for the group to assess vulnerabilities and recommend comprehensive policy to assure continued

---

[46] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., x

[47] Giddens, Anthony. 1999. "Risk and Responsibility". *The Modern Law Review* 62 (1). [Modern Law Review, Wiley]. 3

operations of critical infrastructure. While the executive order was primarily looking for an assessment of current threats, in the opening letter of the PCCIP's report, the Commission dismisses current threats and refocuses on the future. They wrote in their opening letter of the report,

> We found no evidence of an impending cyber attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it.[48]

Although the Commission acknowledged that vulnerabilities could be exploited, they did not believe that the United States was on the brink of experiencing a catastrophic cyber attack. Rather, they believed that threats to infrastructure were real and would continue to grow as a result of increasing 'connectedness' and dependencies on information technologies. This was particularly concerning for the Commission because they find that very little was in place to defend against these increasingly dangerous attacks.

With very little in place to defend against cyber threats that the PCCIP found to be increasingly dangerous, the PCCIP once again emphasizes the need to focus on future threats over current threats. They wrote,

> Physical means to exploit physical vulnerabilities probably remain the most worrisome threat to our infrastructures *today*. But almost every group we met voiced concerns about the new cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyber threats ***before*** they materialize and produce major system damage[49]

---

[48] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., I

[49] Ibid., 5

Although physical threats were the greatest current threat to infrastructure, the Commission downplays their significance. Instead, they emphasize once again (quite literally with bold and italics) the need to develop means for protecting infrastructure from a new and growing cyber threat for the future before catastrophe strikes. Framing risks in this manner is emblematic of risk society. According to Gibbons, "the idea of risk is bound up with the aspiration to control and particularly with the idea of controlling the future."[50] So long as it is in the future, a risk can still be mitigated, controlled, and managed. Consequentially, this framing allows the PCCIP to recommend policy that can have an impact on those risks, giving them some control over the future.

The Commission calls for a change in the understanding of infrastructure protection, writing that their "fundamental conclusion [from the report] is that we have to think differently about infrastructure protection today and for the future."[51] In the new information age, threats to infrastructure were shifting from primarily physical threats to cyber. The conclusion relates to changes in how infrastructure must be understood for future protection. Going forward, the Commission recognized that infrastructure could no longer be thought of as individual units, but rather as systems. The effects of a local infrastructure network breach and outage could cascade to the regional or national level. Beck demonstrates these sorts of effects with the example of an atomic plant, where an 'accident' could affect "even those not yet alive at the time or in the place where the accident occurred"[52] and outlast generations. In both cases, the consequences are far

---

[50] Giddens, 3.
[51] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., vii
[52] Beck, 22

reaching, affecting even those who seemingly have no connection to the incident. Thus, as a result of the interconnected and systemic nature of infrastructure, the Commission

> found that the nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation's security, economic health, and social well-being. In short, they are the lifelines on which we as a nation depend.[53]

The Commission believed that due to the national dependency on infrastructure, cyber vulnerabilities to critical infrastructure had to begin to be viewed as a national security interest.[54] Cyber threats to critical infrastructure had to be treated as potentially catastrophic risks to the state and its security. Thus, the PCCIP's fundamental conclusion that infrastructure protection required different thinking meant that it "must accommodate the cyber dimension"[55] where "there are no boundaries."[56] This same mode of thinking has been applied within risk society. While the report focuses on risks that cyberspace pose to critical infrastructures, framing cyberspace as a dimension that knows no bounds begins to securitize it. This characterization suggests that someday the threat will extend beyond critical infrastructures to other aspects of life. Thus, in order to accommodate the cyber dimension and the future risks it posed, security would be trusted to technical experts who could mitigate risks of future threats before they materialized.

---

[53] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., vii

[54] A later chapter of this thesis will examine the national security framing in further detail, arguing that during the Bush Administration, framing cyber threats to critical infrastructure in terms of national security allowed for the securitization of cyberspace.

[55] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., vii

[56] Ibid.,

Experts' Framing of Cyberspace

While risk society is evident in the PCCIP's report due to its preoccupation with the future, the report further demonstrated risk society through its reliance on experts. In risk society, risks are a result of modernity. The same scientific and technological advancements that enhance society also manufacture new risks. For instance, the science that creates nuclear power plants also creates the risk of radiation exposure. Similarly, the technological advancements that make management of critical infrastructures simplified, efficient, and automated through networks also make them vulnerable to hacking. Thus, as scientific advancement propels us into the future, it also creates "new risk environments for which history provides us with very little previous experience."[57] The risks presented are just as new and cutting edge as the technologies that created them. As a result, "technical experts are given pole position to define agendas and impose bounding premises a priori on risk discourses."[58] The same experts who create the technologies that bring us modernity are used to create the discourse of the risks surrounding modernity. Frequently, the calculation and comprehension of risk is just as complex as the technologies creating them. Giddens writes that in risk society, "we often don't really know what the risks are, let alone how to calculate them accurately in terms of probability."[59] As a result of the uncertainty, experts are used to creating narratives of and about risk that they then make available to the broader public. In other words, experts are authorized to articulate what and how risks are emerging on behalf of the public. This section will convey how the PCCIP conveyed these concepts to the public. First the

[57] Giddens. 4
[58] Beck, 4
[59] Giddens. 4

PCCIP emphasized the complex, technical, and often unknowable nature of the risks and potential harms presented by cyber vulnerabilities. As a result, in order to qualify the risks, the PCCIP connected technical risks to collective referent objects in critical infrastructure.

In its analysis of the risk that cyber threats/ vulnerabilities present to infrastructure, the Commission emphasizes that the risks created by cyber threats are complex and somewhat unknown. According to the Commission, critical infrastructure has always faced physical threats. Infrastructure has been subject to natural threats such as floods, storms, and earthquakes. Consequentially, measures have been developed to protect against these risks and infrastructure operators are able to maintain or quickly restore services.[60] Similarly, man-made threats, such as bombs or arsons, are not new and can be protected against accordingly. Cyber threats, however, make things more difficult. Cyber attacks are more sophisticated, and can "exploit the emerging vulnerabilities associated with the complexity and interconnectedness of our infrastructures."[61] Cyber vulnerabilities blur the lines between infrastructures. Not only can cyber vulnerabilities be exploited to take advantage of a single unit, but the interconnectedness of networks creates dangers of cascading effects where minor outages to escalate into regional outages. Therefore, the effects of a cyber attack "could spread far beyond the radius of a bomb blast."[62] Through this example, the Commission invokes similarities to nuclear radiation, a classic problem of risk society, where there are lingering effects far beyond

---

[60] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., 5
[61] Ibid., 5
[62] Ibid., 5

an attack's initial target. Cyber attacks on a unit of infrastructure are not merely contained events, but can affect units across networks seemingly unconnected to the initial attack. Furthermore, when faced with these vulnerabilities, "technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs."[63] Infrastructure networks are so interconnected and complex, it is hard to determine when these connections create vulnerabilities. As a result, the factors playing into creating risk is presented as both complex and largely unknown. Technical interdependencies of information systems in infrastructure make it so that vulnerabilities may not be fully understood until after they have been exploited. This closes the discussion of cyber related risks off to the public and instead reserves it for experts, who are seen to have the technical understanding to best create the discourse surrounding risk.

Just as the calculation of risk is complex and requires expert knowledge, the understanding of what the harm itself is that is creating the risk within risk society is complex as well. Similar to the risk, the Commission describes the harms as complex and unknown. The Commission writes, "computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways we cannot yet conceive."[64] Technical complexity makes the harm that could be induced by a cyber attack hard to fathom. In risk society, the harm is unknowable because the risk is incalculable. After all, the risks can "induce systemic and often irreversible harm, [but] generally remain invisible [because they] are based on casual interpretations."[65] As an

---

[63] Ibid., x
[64] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., 5
[65] Beck, 22-23

effect of casual interpretation, harm is understood in probability, not possibility. Harm is therefore a function of risk, an already complex and unknown function. Complexity therefore makes the harm difficult for the public to grasp, which in turn reserves its discussion and calculation to experts with the knowledge to comprehend it.

As a result of the complex nature of the factors that create the understanding of both harm and risk, knowledge holds an important role in risk society. Most of the dangers described in risk have never occurred. The risks are results of modernity, and therefore not historical precedent exists for their comprehension. Thus, the risks "initially only exist in terms of the (scientific or anti-scientific) knowledge about them."[66] Certainly this too is the case for risks created by cyber vulnerabilities to critical infrastructure. In the 1990s cyber threats to these infrastructures were fairly new. The Commission emphasizes the technical complexity of the risks because it makes construction less widely available. Technical complexity narrows the authority to qualify risk to technical experts. Certainly, this can help to dispel faulty misconceptions about risk. However, this also allowed the Commission, a Presidentially formed committee that was staffed with high-ranking bureaucrats and industry leaders plus all of their resources, the power to shape the knowledge surrounding cyber risks.

The Commission presented themselves as expert authorities within the report. One method of doing this was emphasizing that as they gathered information to build their report, they used a scientific approach. For instance, the Commission states that they

[66] Beck, 23

> thoroughly reviewed the vulnerabilities and threats facing our infrastructures, assessed the risks, consulted with thousands of experts, and deliberated at length as to how best to assure our nation's critical foundations in the decades to come.[67]

Through this characterization, the Commission presents its insights as scientific and most importantly expert driven and neutral. It is often presumed that a scientific approach provides unbiased knowledge, in this case about the Commission's findings on the state's critical infrastructure protection. Expert knowledge is often the only manner through which risks and their potential harm can be understood. However, even when using a scientific method, experts are creating and then framing the knowledge surrounding risks from cyber vulnerabilities in infrastructure. Specifically, the Commission framed cyber threats to information systems/networks in the context of different collective referent objects. These referent objects included critical infrastructures through which the impact of threats could be understood such as power grids, 911 emergency services, and facets driving the economy.

The PCCIP assesses vulnerabilities to information systems/networks in the context of their analysis of information and communications as a unique sector. According to the Commission, the largest threats facing the information and communications sector were cyber threats due to the fact that the PTN[68] is "increasingly

---

[67] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., 6

[68] The Public Telecommunications Network (PTN) is made up of billions of miles of fibers and cables connecting the country. Phone lines, and large portions of the Internet, rely on it in order to operate. Internet Protocols communicate by breaking data into small packets then transporting them across networks to different routers before reassembling them at their end location. Packets can take different paths; so many packets rely on PTN facilities at some point during their transfer end to end. The Commission analyzes the PTN when looking at 'information and communications' vulnerabilities since it is a collective referent object whose vulnerabilities would have wide ranging effects. I use the

software driven and remotely managed and maintained."[69] This was not a unique characteristic to the PTN, but all information systems and 'connected' devices. However, knowledge of software is inherently technical, and consequentially unavailable to the majority of the public due to technical complexity. By presenting the cause of threat as a result of a shift towards a software driven world, the threat is being presented as a technical threat. Despite the technical nature, the report offers high-level assessments of technical vulnerabilities of networks in areas like switching, signaling, control, and management.[70] While this begins to expose some of the technical knowledge surrounding network vulnerabilities, these more technical assessments are used to argue that a skilled hacker could remotely access or tamper with these elements to create widespread cyber theft or disruptions on networks.[71] Implicitly, this still reserves the knowledge surrounding the calculation and creation of risks to experts. The report therefore presents threats to information and communication via networks as technical, and experts are authorized to explain these risks. Furthermore, when the Commission presents technical details, it is to reinforce threats to critical infrastructures, which have wide reaching impact.

---

quote denoted by the next footnote as a characterization of computer networks even though in the context of the quote they were specifically referring to the PTN

[69] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., A-4

[70] These details are not in the main report, but instead pushed back in the appendix- further demonstrating that the details of what creates the risk need not be consumed by most reading the report.

[71] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., A-8

The Commission is able to connect referent objects and cyber threats by describing risks to information systems. The Commission divides parts of critical infrastructure into five tangible sectors: information and communications, energy, banking and finance, physical distribution, and vital human services. Expert knowledge was used to connect cyber vulnerabilities in these sectors to collective referent objects related to physical and economic security in order to create a clearer concept of risk and harm for the public. For instance, in physical distribution (transportation), NAS, or the National Airspace System that runs all the country's air traffic controls is presented as a target that is "particularly at risk from information-based attacks"[72] as it gets connected other networks. This threat-construction emphasizes how interconnected infrastructure is. Similarly, in energy industries, most vulnerabilities are

> created in the operating environment by the rapid proliferation of industry-wide information systems based on open-system architectures, centralized operations, increased communications over public telecommunications networks and remote maintenance[73]

This characterization is similar to one presented by the Commission for the PTN. Although most critical infrastructure faces similar cyber threats to their networks, experts characterize the threats as threats to the collective referent object, not the technical object, the network. However, at the end of the day, the rapid advancements made in information and computing systems were creating risks for society as a whole through the vulnerabilities in critical infrastructure. The speed at which cyber systems were being adopted in critical infrastructures left risks that undiscovered vulnerabilities could be exploited or result in widespread system failures. Acting as a team of experts, the PCCIP

---

[72] Ibid., A-17
[73] Ibid., A-26

framed these risks in terms of critical infrastructure that could serve as collective referent objects so that these risks could not only be understood by the public but also so that they could be managed.

Cyberspace Technified and Tied to Experts for Understanding

Authority in cyberspace was being shifted out of the hands of policymakers and into the hands of computer scientists and related technical personnel. Describing the risk and defining the harm that that cyber threats presented to critical infrastructure required expert knowledge. The public needed experts to demonstrate that an abstract cyber vulnerability in the information systems of a critical infrastructure asset could lead to tangible harm, like a shutdown of an entire power grid. Similarly, these experts were needed to assess the likelihood that these events could occur. The need for experts to define cyber risk and harm for critical infrastructure caused critical infrastructure protection, and thus cyberspace, to become technified; meaning conceived of as a technical realm that ought to be reserved for experts. Due to their technical knowledge, these experts would be given authority to define cyber threats and frame their impact on security.

Technification was the hallmark of risk society in critical infrastructure. In the introductory section of *Risk Society*[74] the authors/ et al. write that

> the primary risk, even for the most technically intensive activates (indeed perhaps most especially for them), is therefore that of social dependency upon institutions and actors who may well be- and arguably are increasingly- alien, obscure and inaccessible to most people affected by the risks in question.[75]

[74] In the edition of *Risk Society* that I used, an introduction was written by Scott Lash and Brian Wynne, not Ulrich Beck.
[75] Beck, 4

The authors voiced concern that in risk society, the people facing the risk are increasingly separated from its construction. The technical nature of the risks facing infrastructure resulted in public dependence on expert knowledge to construct and present the risk to critical infrastructure in terms of collective referent objects. While the expert knowledge is good in that it makes risks available to the public, it also presents a hazard. Risks

> can thus be changed, magnified, dramatized, or minimized within knowledge, and to that extent they are particularly open to social definition and construction. Hence the mass media and the scientific and legal professions in charge of defining risks become key social and political positions.[76]

Technification does not merely give experts power over matters that are technical, but also political because it cedes power. By framing technical cyber risks in terms of collective referent objects, the Commission constructed the risk in terms that will facilitate political action to address them. However, political authority cannot address the risks without technical expertise, and thus defers once again to the Commission. Consequentially, policy-making authority is also given to experts.

Overall, cyber security, specifically as it relates to critical infrastructure exemplified Beck's concept of risk society. The threats facing critical infrastructure were not framed as current threats, rather they were framed in terms of future risk. In order to manage these risks, technical experts were authorized to frame cyber threats facing critical infrastructure. These experts framed risks in terms of critical infrastructure whose operation was required in the name of the economy and often in the name of national security. However, this framing was not yet in the name of security. Cyber threats were not pressing, or in need of immediate action. Rather, they were framed in a manner where

[76] Beck, 23

they could be managed through technical expertise. Furthermore, these threats were not yet existential threats to the state. However, after September 11th, this would change.

Chapter 2

Just as technology experts were used in order to prevent catastrophe from occurring in critical infrastructure, they were trusted to respond to catastrophe to assure that it would never happen again. In February 2002, a panel of technology consultants testified before Congress. Their testimony sought to show how "their existing data-mining techniques could be put to use in the war on terror."[77] Furthermore, they noted that all the data required to prevent the attacks on September 11th was in place, but stovepiped into different databases. Had "algorithmic search capacities"[78] been in place, the consultants insisted that "9/11 could have been predicted and averted" [79] by identifying the terrorists as potential threats. The system would compile data across sources and platforms then break them down to their core attributes that could be searched for patterns. Once a pattern is identified, certain combinations could be identified then flagged as potential risks. Technology, the consultants believed, could have been used to avert the tragedy, and thus technology should be trusted in the aftermath to manage the risk of future terrorist attacks against the United States.

In the context of risk society, technology cannot necessarily identify risk. While technology can facilitate the screening process and may appear to automate the process of identifying risks, Louise Amoore notes "it is not strictly the case that judgment is replaced by computation but that judgments are made via computation, by the imaginative calculation of the possibility, and not the strict probability, of a future

---

[77] Amoore, Louise. Politics of Possibility : Risk and Security Beyond Probability. Durham: Duke University Press, 2013., 41.
[78] Ibid., 41.
[79] Ibid., 41.

event."[80] The technology replaces judgment with computation, but computation does not inherently produce neutral judgment. Yet, in the wake of 9/11 the role of the technologist and technology were portrayed in this manner. The case of technology in airport security was an example of a broader shift occurring within American society. These technologies were seen as an unbiased means through which threats could be identified and prevented in cyberspace as well.

After September 11th, terrorism was viewed as an immediate and present danger to the security of the United States. In light of this new danger, the US was increasingly turning to technologists promising to create technical solutions that could identify threat and guarantee security. While technology could be used to mitigate risk, it was increasingly becoming the threat- especially in the realm of the digital economy. Many feared that terrorists could use these technologies to cause harm. As threats became increasingly technical, so did the means through which they could be prevented. Technical experts that were previously trusted to identify risk therefore became trusted to ensure security due to their knowledge of technical systems that were beyond the comprehension of the general public. Thus, as threats became increasingly technical, security started to become technified, or reliant upon experts for understanding.

This chapter will argue that cyberspace became securitized in the aftermath of September 11th. First, the chapter will analyze policies of the Bush Administration in October 2001 to protect critical infrastructure from terrorism. Policies shifted from thinking of cyberspace as being at risk in the future to something that was an existential and immediate threat and thus needed to be addressed immediately. This was achieved by

[80] Ibid., 50.

expanding the definition of critical infrastructure while explicitly connecting infrastructure to national security threats. Additionally, these policies created expert organizations in order to secure critical infrastructure in the name of national security. Under the new understanding of critical infrastructure created by the Patriot Act, expert organizations emphasized the connection between cyberspace and critical infrastructures. Furthermore, these organizations emphasized the threats to the public while developing plans to secure them. The final result was *The National Strategy to Secure Cyberspace*, a report that securitized cyberspace.

In October 2001, the Bush Administration created a number of policies to secure the nation from terrorism. Many of its actions focused on securing critical infrastructure, an area where cyber vulnerabilities had been identified in the previous presidential administration. However, differences existed between these Administrations' treatment of critical infrastructure vulnerabilities. While the Clinton Administration viewed vulnerabilities to critical infrastructure through the lens of risk, the Bush Administration saw these vulnerabilities to critical infrastructure through the lens of national security. Thus, under the Bush Administration, cyber threats are addressed and considered with in greater urgency. Consequentially, the Bush Administration securitized critical infrastructure through means such as the Patriot Act and the Office of Homeland Security.

The Patriot Act

The USA Patriot Act was passed by Congress and signed into law in October 2001 with the intent of strengthening security measures to protect against terrorism. The Patriot Act achieved this primarily by expanding the powers of law enforcement and

federal agencies. While expanding security and counterterrorism measures were the primary focus of the bill, it also expanded the definition of critical infrastructure as well. Under the Clinton Administration, critical infrastructure had defined as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[81] Comparatively, the Patriot Act expanded the definition of critical infrastructure under the Bush Administration to

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[82]

The definition of critical infrastructure changed from minimal to expansive. Critical infrastructures were expanded from the systems guaranteeing minimum operation of government and economy to systems that have impacts on health, safety, or national security.

The definitional change signaled a shift in two related but distinctly important ways. First, obstructions to critical infrastructure were no longer framed primarily as economic issues, but security issues. The Patriot Act therefore demonstrated that the Bush Administration would view threats to critical infrastructure as threats to national security. Second, the Patriot Act allowed all physical and virtual systems 'vital to the United States' that could have an impact on national security to be understood as critical infrastructure. As a result of these changes to the definition of critical infrastructure, cyberspace would become securitized. However, cyberspace was securitized through an

---

[81] Clinton Administration, Presidential Decision Directive 63 (PDD-63): Policy on Critical Infrastructure Protection (May 22, 1998)

[82] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Public Law 107–56, 107th Congress, October 26, 2001., Sect 1016e.

interesting dichotomy. Although cyberspace was the existential threat to critical infrastructure, it simultaneously was a referent object that needed to be secured.

Cyber vulnerabilities that existed in critical infrastructure would no longer merely be considered a risk as they were by the Clinton Administration, but an impending threat that could impact national security. Hence, cyberspace and the potential vulnerabilities it created in critical infrastructures was the threat to national security. However, cyberspace was also a referent object that needed to be secured. After all, cyberspace was increasingly becoming 'vital' to the American way of life, and could be considered a critical infrastructure to the United States in its own right. The next chapter of this thesis will later examine this further through an analysis of *The National Strategy to Secure Cyberspace*, arguing that the connection between critical infrastructure and cyberspace was key to the securitization process.

Expert Organizations

As the understanding of critical infrastructures was expanded under the Patriot Act, President George W. Bush created a number of organizations to serve as experts to help secure digital infrastructure and information systems of critical infrastructures from threats. On October 8, 2001, President Bush established the Office of Homeland Security (which became the Department of Homeland Security the following year). Homeland Security's primary mission was to protect America from terrorist attacks,[83] portrayed as a top threat to American national security in the wake of September 11th. As part of their mission, the Office of Homeland Security would be tasked with protecting critical infrastructure. Homeland Security would "coordinate efforts to protect critical public and

[83] Executive Order 13228—Establishing the Office of Homeland Security and the Homeland Security Council. Federal Register, Vol. 66, No. 196, October 8, 2001. Sect 2

privately owned information systems within the United States from terrorist attack"[84] and "coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack."[85] By empowering the Office of Homeland Security to protect critical infrastructure within their efforts to protect America from terrorist attack, the government implicitly acknowledged that critical infrastructures could be vulnerable to the threat of terrorist attacks. The creation of Homeland Security and their broad powers to coordinate efforts over critical infrastructure in order to protect the United States from terrorist attacks therefore aided in the securitization of critical infrastructure. This would eventually consolidate the securitization of cyberspace.

In order to support the Office of Homeland Security with their missions in infrastructure protection, President Bush established the President's Critical Infrastructure Protection Board (PCIPB)[86] and the National Infrastructure Advisory Council (NIAC) comprised of up to 30 expert members appointed by the President from the private sector, academia, and state/local government.[87] Both groups would develop cyber infrastructure protection, with the PCIPB coordinating at a federal level while the NIAC would coordinate cooperation between public and private sectors. Additionally, the

---

[84] Executive Order 13228—Establishing the Office of Homeland Security and the Homeland Security Council. Federal Register, Vol. 66, No. 196, October 8, 2001 Sect Eii
[85] Ibid., Sect Fii.
[86] Note: The President's Critical Infrastructure Protection Board (PCIPB) is also referred to as 'the Board' within this paper. Other sources will refer to this organization on occasion by a similar acronym (CIPB), leaving off the first P
[87] Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age. Code of Federal Regulations, title 3 (2001). Sect 10b

executive order calls for the Board to propose a National Plan in coordination with Homeland Security on matters related to infrastructure protection.[88]

Similar to President Clinton and his President's Commission on Critical Infrastructure Protection (PCCIP), President Bush created expert organizations to evaluate vulnerabilities to critical infrastructure and aid in policy development. However, President's Bush's organizations were distinct. While President Clinton's PCCIP was tasked to "assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures"[89], Bush's organizations were to "secure information systems for critical infrastructure."[90] The contrasts between these two statements are notable for a number of reasons.

First, the initiatives of these respective groups changed from passive to active. While the PCCIP under Clinton would assess, the organizations created under Bush would secure.[91] This change is significant because it demonstrated that critical infrastructure protection was no longer just a question of risk. Through September 11, the threat of terrorism had been realized and the harm had been done. Terrorists had demonstrated their willingness to go to great lengths in order to inflict harm upon the general population within in United States. Harm was no longer an uncertain calculation, it was witnessed firsthand. The 2003 report *The National Strategy to Secure Cyberspace* noted that in the aftermath of the attacks, "the federal government and society as a whole

---

[88] Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age. Code of Federal Regulations, title 3 (2001). Sect 9a
[89] Executive Order 13010 of July 15, 1996, Critical Infrastructure Protection. Code of Federal Regulations, (1996): Sec C
[90] Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age. Code of Federal Regulations, title 3 (2001). Sect 1a
[91] Later organizations, such as US Cyber Command, would not just act in defense to secure but also would hold offensive capabilities

[were] forced to reexamine conceptions of security on home soil."[92] If critical infrastructures were vulnerable, certainly terrorists would try their best to exploit them. As a result, critical infrastructure vulnerabilities no longer needed to be assessed as for future risks, but instead needed to be actively secured from a present terrorist threat. The shift from passive to active in the role of experts who were charged by the President with protecting critical infrastructure demonstrated that cyber vulnerabilities in critical infrastructure had shifted from future risk to active threat.

Additionally, the difference in the mission statements between the Clinton Administration and the Bush Administration emphasized the shift from protecting critical infrastructures themselves to protecting the information systems of critical infrastructure. While Clinton's PCCIP would generally assess 'vulnerabilities of, and threats to, critical infrastructure', Bush's PCIPB would specifically focus on 'information systems for critical infrastructures.' Therefore, information systems were of greater concern to the Bush Administration than they had been to the Clinton Administration. The PCCIP had foreshadowed this shift in their 1996 report, which said that the day would come when cyber threats (which impact information systems) would pose a greater danger to infrastructure than physical threats.[93] The emphasis on securing information systems of critical infrastructure demonstrated that that day had in fact come and cyber vulnerabilities were of greater concern. Furthermore, the Board, established to aid in policy creation for critical infrastructure protection, was to be chaired by the Special Advisor to the President for Cyberspace Security; a position often referred to as the

---

[92] *The National Strategy to Secure Cyberspace* pg 5

[93] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997., 5

Cyber Security Czar.[94] While the Administration's Cyber Czar would have knowledge of securing information systems, his leadership over the Board signaled that securing critical infrastructure by 'securing information systems for critical infrastructures' would include securing cyberspace more broadly. The Board recognized this point, noting in a 2003 report that the US "economy and national security became fully dependent upon information technology and the information infrastructure on which it runs."[95] These information systems, which made up cyberspace, were starting to become considered critical infrastructure in their own right. After all, the understanding of critical infrastructures had been expanded under Patriot Act to systems "so vital to the United States"[96] that their incapacity would impact security. Cyberspace, through its information systems, was declared vital to the security of the United States. Consequentially, cyberspace became part of national security. While cyberspace had previously been thought of as a potential risk, cyberspace and its vulnerabilities were now thought of as an external threat to national security. Furthermore, this shift led to the creation of expert organizations to secure the information systems of critical infrastructures. Ultimately this caused the securitization of cyberspace. Moreover, these bodies of specialists were tasked with making cyber infrastructure policy, reinforcing the securitization of cyberspace through technification.

---

[94] Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age. Code of Federal Regulations, title 3 (2001). Sect 7a

[95] *The National Strategy to Secure Cyberspace*. Washington, D.C.: Dept. of Homeland Security, 2003., 6

[96] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Public Law 107–56, 107th Congress, October 26, 2001. Sect 1016e.

Soon after their creation, these organizations began the process of making policy. Operating in coordination with Homeland Security, the President's Critical Infrastructure Protection Board got to work creating a national strategy. Critical infrastructure protection would be broken into two parts: physical infrastructure (which included key assets) and cyber infrastructure.[97] Under the leadership of Cyber Czar Richard Clarke and Vice-Chairman Howard Schmidt, the Board's efforts focused on cyber infrastructure protection. The Board's national plan, titled *The National Strategy to Secure Cyberspace*, would be created through a unique collaborative process using a public-private partnership. The Board emphasized that the private industry had an important role to play in the protection of cyber infrastructure. As Tom Noonan, President and Chief Executive of Internet Security Systems noted, ""The protection of our national online infrastructure is significant in that it marks the first national security issue our government cannot handle alone."[98] Much of the infrastructure on which cyberspace relied was privately owned and operated. As a result, any efforts towards governance over the cyberspace, even in the name of security, would require partnership between public and private actor in order to be effective. Along with being developed as a public private partnership, the strategy would also be a living document. The document was not intended to be static, rather the document would continually be updated and refreshed in order to adapt to a changing environment.[99]

---

[97] *National Strategy for Homeland Security*. Washington, D.C.: Office of Homeland Security, 2002., 33

[98] Internet Security Systems. "Internet Security Systems Chairman, Tom Noonan, to Participate In White House Town Hall Meeting on Cyber Security." PR Newswire. July 2002.

[99] Bennett, Amy. "UPDATE: US Drafts National Strategy to Secure Cyberspace." ITworld. September 18, 2002.

As a collaborative creation developed through a public private partnership, the strategy gathered input in two ways. First, the Board conducted extensive research, including meeting with industry leaders, security experts, academics, and members of state and federal government for input and recommendations.[100] These professionals would help identify the major concerns and areas that needed to be focused on. This helped to shift the role of defining security from traditional military and foreign policy analysts to technologists. Second, while gathering information from professionals, the Board would take input from the public in two forms. As drafts of the strategy were released, the Board provided the public with a means for providing comments on the strategy online or by mail.[101] Additionally, as drafts of their strategy were being developed, the Board hosted ten town halls in different cities around the country.[102] According to President Bush's letter in the final report, the purpose of these town halls was "to gather input on the development of the strategy."[103] While the town halls were designed as a way to allow the public to give input for *The National Strategy for Securing Cyberspace*, they also served as an opportunity for the President's Critical Infrastructure Protection Board and the newly created Department of Homeland Security to convince the public of the threat from cyberspace.

---

[100] Bennett, Amy. "UPDATE: US Drafts National Strategy to Secure Cyberspace." ITworld. September 18, 2002.

[101] President's Critical Infrastructure Protection Board, Executive Office Of the President, The White House. "Notice of pending request for public comment regarding the National Strategy to Secure Cyberspace for comment". Federal Register, Vol. 67, No. 201, October 17, 2002.

[102] Information on these town halls was difficult to find. The author could not locate transcripts or video of these town halls. Uncovering this in future research could strengthen the argument made in this project

[103] *National Strategy to Secure Cyberspace*, iii

The town halls hosted by the President's Critical Infrastructure Protection Board were events open to the public that would focus on creating a dialogue between the American public and professional panel on the new national strategy. Along with a senior member of the Board, like Chairman Richard Clarke or Vice-Chairman Howard Schmidt, the panels usually consisted of a mix of industry leaders, academics, and high-ranking government officials. Numerous other organizations participated in these town halls by sponsoring them including universities, think tanks, professional associations and various private firms in cyber security and defense contracting. An event description for a town hall in Atlanta wrote, "this event will provide an opportunity to raise awareness of the need for cyber security, and educate Americans on current cyberspace security initiatives."[104] While President Bush had described the town halls as a means for the Board to gather input, the event description portrays the event as a lecture. The town halls were less of a conversation and more one-sided. While the public would get to engage the panels with questions, the purpose of the town hall was for panelists to 'educate' the public and 'raise awareness' on cyberspace security. Panelists used these town halls as an opportunity to educate the public on the increasing threats in cyberspace and convince them on the need for action.

In securitization, the securitized audience plays a crucial role. This audience determines whether or not a securitization will be successful by accepting or rejecting a securitizing narrative. When they agree with the message of the securitizing actor, an issue is accepted as a threat. Once an issue is accepted as a threat, in the name of security

---

[104] Internet Security Systems. "Internet Security Systems Chairman, Tom Noonan, to Participate In White House Town Hall Meeting on Cyber Security." PR Newswire. July 2002.

action becomes warranted. In their study of securitization in cyberspace, Hansen and Nissenbaum note that the securitizing actors' narratives are particularly salient in cyberspace.

> cyber security discourse moves seamlessly across distinctions normally deemed crucial to Security Studies: between individual and collective security, between public authorities and private institutions, and between economic and political-military security.[105]

The securitization affects a wide reaching audience because the threat is not concentrated in one single level but instead has implications on numerous levels of security. Cyber security has implication ranging from the individual to the nation state. The town hall panelists utilized this insight during town halls to strengthen their securitizing narrative while encouraging people to secure their portion of cyberspace. For instance, in the process of describing the dangers facing national online infrastructure, panelist Tom Noonan of Internet Security Systems said,

> Today's threats are much more complex and destructive than ever before and do not discriminate among home users, small businesses, large enterprises and government organizations-putting our citizens, businesses and government at risk.

Noonan, speaking from a position of expert authority as a panelist on a PCIPB town hall, frames dangers in cyberspace not only as a threat, but a threat that is destructive, implying real harm. Furthermore, the threat is widespread in its reach. According to Noonan's description, the threat impartially covers various levels and types of users, leaving very few unaffected. Not only does this dialogue present risks in cyberspace as a matter of security, but as a matter of security at numerous levels for various audiences.

In addition to securitizing cyberspace, the town halls also taught Americans how to secure their cyberspace. After laying out the various threats the nation faced in

---

[105] Hansen and Nissenbaum, 1161

cyberspace, the panelists discussed with participants "what they can do to protect our nation's infrastructure."[106] After presenting the audience with a wide range of threats that they faced in cyberspace, panelists provided the public with immediate actions they could take to secure cyberspace. The panels, and later the report, focused on doing this in order to "empower every American to secure their portion of cyberspace."[107] This was focused on five levels, many of which were mentioned by Noonan: home-users and small businesses, large enterprises, sectors of the economy, national issues and vulnerabilities, and global. Town halls were tailored to the general public, and as a result covered ways to secure cyberspace for citizens, business, and government at various levels. Yet, through these levels, the panel could make a threat relevant to each audience member in some way while demonstrating that they could offer a solution. Thus, the town halls purpose was twofold. In the words of Richard Clarke, town halls "give all Americans the opportunity to discuss this important issue and to allow us to share ideas of securing America's cyberspace."[108] Town halls allowed the President's Critical Infrastructure Board to securitize cyberspace by enabling experts to serve as securitizing actors who presented the narrative of cyber threats to the public. While the town halls were intended to create a dialogue about the strategy, the town halls served as a stage to present the securitization to public through these types of narratives in order to persuade them of the threats existing in cyberspace. Additionally, these experts' ability to offer solutions to

---

[106] Kimberland, Kelly. "Carnegie Mellon Hosts White House Meeting on Cybersecurity." *Carnegie Mellon Views*, December 2002.
[107] Kimberland, Kelly. "Carnegie Mellon Hosts White House Meeting on Cybersecurity." *Carnegie Mellon Views*, December 2002.
[108] Internet Security Systems. "Internet Security Systems Chairman, Tom Noonan, to Participate In White House Town Hall Meeting on Cyber Security." PR Newswire. July 2002.

mitigate threats for different levels further legitimized their authority to persuade audiences to accept their securitizing narrative.

In February 2003, Homeland Security released both *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and *The National Strategy to Secure Cyberspace*. While the former would focus on protecting critical infrastructures from physical attacks, the latter would focus on "protection of interconnected information systems and networks."[109] These two reports were to serve as complements, "form the road ahead for one of our core homeland security mission areas." Neither document was binding law; rather they were strategies for securing. Nevertheless, in the case of *The National Strategy to Secure Cyberspace*, the initiative served as an opportunity for the government to begin to move into cyberspace and its governance in the name of security. Not only does this mean that the securitization is successful, but it also authorizes the state power by allowing the state to act to secure society against cyber threats.

[109] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, D.C.: Dept. of Homeland Security, 2003., 2

Chapter 3

This chapter will analyze *The National Strategy to Secure Cyberspace* from February 2003 to demonstrate that cyberspace became incorporated into the understanding of critical infrastructures, and consequentially became a matter of national security. As a result, *The National Strategy to Secure Cyberspace* securitizes cyberspace. The securitization connected cyberspace to critical infrastructure in two ways. First, cyberspace is connected to critical infrastructure due to the dependence of critical infrastructures on cyber information systems. Second, cyberspace is presented as critical infrastructure itself due to the nation's dependence upon cyberspace. Through these connections, cyberspace is portrayed as a threat to critical infrastructures due to technical vulnerabilities in the networks that operate critical infrastructure. Yet, cyberspace is also portrayed as a vulnerable referent object that is critical infrastructure and needs to be secured. However, in both cases, the threat of cyberspace and the threats facing cyberspace were presented as technical. This in turn implied that explaining the role for cyberspace was reserved for experts. The chapter will argue that technification strengthened the securitization of cyberspace by legitimizing it while making it appear to be politically neutral. People accept technology as inherently neutral and thus accept technical assessments as neutral. Furthermore, technification gives experts the power to frame security in cyberspace: creating the reality through which threats, security, and proper responses in cyberspace are understood. As a result of this technocratic framing, the political stakes of decisions being made in the name of security are often overlooked. The chapter will conclude by demonstrating the implications that technification has on the ability to control the frame within which the cyber realm is discussed. Thus, *The*

National Strategy to Secure Cyberspace reinforces the securitization of cyberspace through technification.

After over a year of research, ten town halls, and numerous drafts, the President's Critical Infrastructure Protection Board released their finalized report of *The National Strategy to Secure Cyberspace* in February 2003. *The National Strategy to Secure Cyberspace* was intended to serve as blueprint that could allow citizens, government, and business to understand security within cyberspace. Furthermore, *The National Strategy to Secure Cyberspace* was given three strategic objectives from the Department of Homeland Security, which DHS outlined in their 2002 report *National Strategy for Homeland Security*. These objectives were:

- Prevent cyber attacks against America's critical infrastructures;
- Reduce national vulnerability to cyber attacks; and
- Minimize damage and recovery time from cyber attacks that do occur[110]

The strategy would outline cyber threats to critical infrastructure as well as threats within cyberspace more broadly while examining ways to minimize damage and recovery time. In order to meet these objectives, the report articulates five national priorities for cyberspace security:

I. A National Cyberspace Security Response System;
II. A National Cyberspace Security Threat and Vulnerability Reduction Program;
III. A National Cyberspace Security Awareness and Training Program;
IV. Securing Governments' Cyberspace; and
V. National Security and International Cyberspace Security Cooperation.[111]

---

[110] *The National Strategy to Secure Cyberspace*. Washington, D.C.: Dept. of Homeland Security, 2003., viii
[111] *The National Strategy to Secure Cyberspace,* x

These national priorities would roughly fall within the objectives laid out by the Department of Homeland Security. For instance, Priority 1 would help to reduce damage, recovery time, and response to cyber incidents; Priority 2-4 would aim to reduce threats from cyber attacks and Priority 5 would seek to prevent cyber attacks to national security assets like critical infrastructures. Within each of the five priorities, *The National Strategy to Secure Cyberspace* proposes actions and initiatives that could be undertaken. However, within the report's objectives, priorities, and proposed actions, *The National Strategy to Secure Cyberspace* advances a narrative that securitizes cyberspace. The report portrays cyberspace as an arena from which threats emerge or is itself insecure. In turn, other ways of thinking about cyberspace, such as a realm for social interaction and public forum, are ignored or silenced. Additionally, the report seeks to technify cyberspace by making it a technical realm reserved for technical experts to comprehend. These experts are then trusted to frame threats for the public so they may understand the urgency and need to immediately address them. The first way which *The National Strategy to Secure Cyberspace* achieves this securitization is by categorizing cyberspace as a threat to critical infrastructures.

Characterizing Cyberspace as a Threat

The National Strategy to Secure Cyberspace establishes cyberspace as a threat to critical infrastructure. This begins as early as the opening letter of the report, written by President George W. Bush. In the opening letter, President Bush writes that US policy will

> protect against the debilitating disruption of the operation of information systems for critical infrastructures [to] help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these

> threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures.[112]

Although the report is titled *The National Strategy to Secure Cyberspace*, the emphasis was placed on critical infrastructure. President Bush stresses the significance of critical infrastructures, as the people, the economy, and most importantly national security rely upon their operation. However, these critical infrastructures were becoming increasingly reliant upon cyber systems, including information systems and networks, for their operation. Consequentially, failure of these information systems or damage as a result of cyber vulnerabilities to these technologies could lead to failure of critical infrastructures. Technological failures in critical infrastructures would have repercussions not only for the people and the economy, but also for national security. Thus, even at the beginning of *The National Strategy to Secure Cyberspace*, the President begins to frame critical infrastructure vulnerabilities as a technical threat with implications for national security.

President Bush further framed cyber vulnerabilities in terms of national security by implying that these vulnerabilities could be 'exploited' or taken advantage of purposefully. Cyber vulnerabilities could 'exploited' by a targeted attack in order to damage the nation's critical infrastructure and harm the United States. As a result, these critical infrastructures need to be protected from cyber vulnerabilities, which Bush presents as a threat to national security. This framing, set forth from the very beginning of the report by President Bush, would be prevalent throughout the report. In addition to framing cyber threats in terms of national security, cyber threats are also presented as technical. For instance the report writes,

---

[112] *The National Strategy to Secure Cyberspace*, iii

> Uncertainties exist as to the intent and full technical capabilities of several observed attacks […] What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving.[113]

Through this characterization, the threats presented by cyberspace are technical, yet increasingly urgent. Additionally, *The National Strategy to Secure Cyberspace* frames the design of cyberspace and the Internet as a threat to critical infrastructures. While this framing presents cyberspace as a threat, it also makes the source of the threat technical and therefore unavailable to the public. Additionally, it ignores the human element of cyberspace, the users. Through this framing, discussion occurs in terms of technology despite the fact they have implications beyond. Thus, the securitization relies on technification to create the threat.

Within *The National Strategy to Secure Cyberspace*, cyberspace is presented as a technical threat to critical infrastructure. *The National Strategy to Secure Cyberspace* presents cyberspace as a technical threat due to its design, which the report implies makes cyberspace inherently vulnerable. These vulnerabilities from cyberspace's design act as a threat to critical infrastructure, which in turn have implications for on national security. *The National Strategy to Secure Cyberspace* does this through its characterizations of the Internet. For instance, the report describes the Internet as

> a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work.[114]

---

[113] *The National Strategy to Secure Cyberspace*. Washington, D.C.: Dept. of Homeland Security, 2003., viii

[114] *The National Strategy to Secure Cyberspace*. Washington, D.C.: Dept. of Homeland Security, 2003., viii

The report implies that the Internet, which connects to most critical infrastructures, was not intended to grow to the scope and scale of today and is therefore insecure. The Internet grew out of ARPANET, a network originally created for a small group of ARPA scientists to share research. These ARPA researchers knew each another and trusted one another well enough not to worry about others 'abusing' the network. In light of this, the report emphasizes that while the Internet's purpose and users have drastically changed, 'that same Internet' is relied up by a majority of vital services and critical infrastructures today.

The characterization of the 'same Internet' creates a sense of vulnerability, because 'that same Internet' has drastically changed since its inception in the early 1980s. The Internet has been scaled up by billions of times since its inception when it first created as a small network for researchers. The Internet has grown from a small network of scientists into a complex web of millions of networks that are both publically and privately held. As the size of the Internet has grown, the size of the user base has as well. The Internet is no longer reserved for academics in research, but available to the public to be used for a wide range of purposes. As a result, it can no longer be assumed that all Internet users are trustworthy and 'uninterested' in abusing networks. Yet, despite the drastic differences since its creation, the excerpt writes 'that same Internet' used by researchers in the 1980s is used today to control critical infrastructures. Through this characterization, the excerpt implies that the Internet's design may be outdated and technologically insufficient for the modern Internet. Since critical infrastructures rely on networks and information systems, these Internet vulnerabilities from technological deficiencies could leave critical infrastructures vulnerable. Thus, *The National Strategy to*

Secure Cyberspace's characterization supports President Bush's argument in the opening letter of the report that cyberspace presents a threat to critical infrastructure. Additionally, by suggesting that vulnerabilities may result from elements of the Internet's structure and design, the report is categorizing the threat as technical. Debates about this technical threat are unavailable to most without a technical background or understanding of Internet design and structure. Thus, by describing the threat as technical, it becomes reliant on experts for understanding. While the public understands that the Internet's scale and user base has changed, few understand the effect of these changes on the security of the Internet.

In addition to describing information systems in critical infrastructure connected to the Internet as vulnerable due to the Internet's design, *The National Strategy to Secure Cyberspace* presents the critical infrastructure's information systems as vulnerable to attack. In addition to increasing the urgency of the threat, the characterization once again implicates the Internet as a source of threat because of its design and structure. Furthermore this representation presents the threat as technical. The report writes,

> By exploiting vulnerabilities in our cyber systems, an organized attack may endanger the security of our Nation's critical infrastructures. The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet.[115]

Once again, the excerpt draws upon the connection between critical infrastructure and cyberspace. Cyber vulnerabilities are portrayed as a threat due to their ability to compromise the security of critical infrastructures, which, as President Bush noted in the opening letter, then have implications on national security. However, this account takes

---

[115] *The National Strategy to Secure Cyberspace*. Washington, D.C.: Dept. of Homeland Security, 2003., xi

cyber vulnerabilities a step further by describing vulnerabilities as an active threat. The report writes that cyber vulnerabilities could be exploited in an 'organized attack' to purposely threaten the security of the nation's critical infrastructures. In this context, the reference to 'organized attack' alludes to terrorism. This is not particularly surprising in the context of the report, after all the Department of Homeland Security, the organization that oversaw the creation of *The National Strategy to Secure Cyberspace*, was created by President Bush to secure America against the threat of terrorism. However, the suggestion that terrorists could exploit cyber vulnerabilities to threaten critical infrastructures is part of the securitizing process and invokes national security. This was a particularly powerful securitizing narrative in the early 2000s as the United States began its War on Terror. Furthermore, an organized terrorist threat against the United States would warrant immediate action or response in order to defend against it.

In addition to evoking terrorism while framing cyber vulnerabilities as a threat to critical infrastructure, the excerpt links the cyber vulnerabilities threatening critical infrastructures to cyberspace more broadly while conveying the threat as technical. The excerpt writes that vulnerabilities in external supporting structures such as 'mechanisms of the Internet' are amongst the greatest threats to critical infrastructures. While this further establishes the Internet as a threat to critical infrastructure, it also reinforces that the threat is technical. The word 'mechanism' itself begins to imply technical machine like qualities. The mechanisms of the Internet specifically are technical aspects that make the Internet run such as protocols, structure, and design. These mechanisms are primarily code. As a result, they are beyond the comprehension of most without a technical background or expertise. Therefore, the average person does not have a deep

understanding of what these mechanisms of the Internet are, what they do, how they make the Internet work or why they could make the Internet vulnerable. Rather, threats regarding mechanisms of the Internet are merely thought of as technical, and trusted to experts. When technical aspects are made available to the public, experts can frame public understanding of the issue in a manner that supports their proposed solutions. As Butler notes, this means that the public is "being recruited into a certain framing of reality"[116] surrounding the issue since they are reliant on experts for its very construction. As a result, when *The National Strategy to Secure Cyberspace* suggests that mechanisms of the Internet pose a threat to critical infrastructure, the threat becomes thought of as technical and therefore reserved for experts for proposing solutions.

In summary, *The National Strategy to Secure Cyberspace* frames cyberspace as a technical threat to critical infrastructures because "cyberspace provides a means for organized attack on our infrastructure from a distance."[117] Furthermore, cyberspace is portrayed as a threat due to the design and mechanisms of the Internet that leave vulnerabilities for attackers to exploit. This technifies the threat, making its understanding unavailable to the public without experts who are trusted to constitute and diagnose the appropriate response in their place.

The National Strategy to Secure Cyberspace also frames cyberspace as a threat to critical infrastructure. As a threat to critical infrastructure, actions must be taken so that cyber vulnerabilities are diminished. While framing cyberspace as a threat to critical infrastructure portrays critical infrastructure as the referent object needing protection, framing critical infrastructure as the referent object makes securing cyberspace only

---

[116] Butler, xii
[117] *The National Strategy to Secure Cyberspace,* 6

necessarily in so far as it affects critical infrastructures. Consequentially, in addition to portraying cyberspace as a threat to critical infrastructures, *The National Strategy to Secure Cyberspace* also frames cyberspace itself as critical infrastructure that needs protecting.

Characterizing Cyberspace as Vulnerable to Threats

In addition to describing cyberspace as a threat to critical infrastructure, *The National Strategy to Secure Cyberspace* also describes cyberspace as a space that is threatened. The report describes cyberspace as a referent object once again by relating cyberspace to critical infrastructure. However, instead of describing cyberspace as a threat to critical infrastructure, the report presents cyberspace as a system that is so vital to the United States' people, economy, and national security that it is considered a critical infrastructure in its own right. Cyberspace is described as a space that needs to be secured from threats. Furthermore, cyberspace is described as a uniquely technical referent object that can be secured by experts with technical expertise. This characterization relies on technification, which ultimately makes the securitization appear politically neutral since it is presented as an extension of technology and separate from human agency.

The National Strategy to Secure Cyberspace uses technification to reinforce cyberspace as critical infrastructure. This characterization involved presenting cyberspace as infrastructure itself in order to make 'securing' cyberspace politically neutral. This begins as early as the introductory letter of *The National Strategy to Secure Cyberspace.* In the introductory letter, President Bush begins the process of describing cyberspace as infrastructure. Bush writes,

> The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network

> of information technology infrastructures called cyberspace. *The National Strategy to Secure Cyberspace* provides a framework for protecting this infrastructure that is essential to our economy, security, and way of life.[118]

Similar to the rest of the report, President Bush describes cyberspace in terms related to critical infrastructure. In fact, President Bush writes that cyberspace is an infrastructure. Furthermore, as an infrastructure President Bush writes that cyberspace needs to be protected since it impacts the economy, security, and American way of life. Bush establishes cyberspace as a referent object, which itself needs to be protected. Along with describing cyberspace as an essential infrastructure, Bush presents cyberspace as a tangible structure made up of technical components. He does this by defining cyberspace 'an interdependent network of information technology infrastructures.' Through these terms, it is implied that cyberspace is technical. Ultimately, this description results in technification.

In his opening letter, President Bush begins to classify cyberspace as technical infrastructure. As President of the United States, Bush writes from a position of high authority. Thus, when he describes cyberspace as technical, it aids the technification. Furthermore, it gives the perception that cyberspace can be secured by technical experts. Physical infrastructures, like dams, power plants, etc., can be secured by physical means (walls, guards, gates, moats, etc). For these types of infrastructures, measures can be put into place to guarantee their protection from threat. Thus, this narrative suggests that technical infrastructure, like cyberspace, can be secured from threat by using technical means. This creates a need for experts, and would ultimately allow *The National Strategy to Secure Cyberspace* to propose the use of technical experts and solutions to protect

---

[118] *The National Strategy to Secure Cyberspace*. Washington, D.C.: Dept. of Homeland Security, 2003., iii

against the technical threats and secure cyberspace. Additionally, technification ultimately makes the act of securing cyberspace appear politically neutral by presenting actions as merely technical solutions. A later section of this chapter will cover this in greater detail.

The National Strategy to Secure Cyberspace builds on President Bush's description of cyberspace from the opening letter of the report by portraying cyberspace as a space that is vulnerable to threats. On the first page of the detailed report, *The National Strategy to Secure Cyberspace* provides a lengthy definition of cyberspace. While the account emphasizes critical infrastructures' reliance on cyberspace, it also begins to describe cyberspace itself as threatened. The report writes,

> Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. Unfortunately, recent events have highlighted the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them.[119]

Cyberspace plays an important role in most critical infrastructures, serving as a nervous system of networks that allows the critical infrastructures of the United States to function. However, this widespread reliance on cyberspace allows cyberspace to begin to be thought of as critical infrastructure itself. For instance, the passage reiterates a point made by President Bush in his opening letter by emphasizing that cyberspace is 'essential to our economy and our national security.' Through both descriptions, cyberspace is portrayed as a critical infrastructure according to the definition under the Patriot Act. The Patriot Act expanded the definition of critical infrastructures to "systems and assets

---

[119] *The National Strategy to Secure Cyberspace,* 1

[which, if incapacitated] would have a debilitating impact on security, national economic security, national public health or safety."[120] Through this understanding of critical infrastructure, cyberspace is more than merely a system that is related to critical infrastructure; rather, cyberspace can be conceived of as critical infrastructure itself. This characterization is common throughout the report. For instance, another section of the report emphasizes the difficulty of securing "the infrastructure that makes up cyberspace"[121] due to its global reach. However, this characterization still classifies cyberspace as infrastructure, and as a critical infrastructure, cyberspace could be secured within the broader effort to protect critical infrastructure. Certainly the report's title, *The National Strategy to Secure Cyberspace*, reinforces this point. The report was originally intended to secure cyber systems of critical infrastructure. However, describing cyberspace in general as a critical infrastructure allows cyberspace to be secured in the name of protecting America's critical infrastructures.

By describing cyberspace as critical infrastructure, cyberspace is added to a group of referent objects that are threatened. However, amongst this group, cyberspace is uniquely described as an infrastructure that is technical. The excerpt supports this perception by describing cyberspace in terms of technical hardware components such as 'computers, servers, routers, switches, and fiber optic cables.' By describing cyberspace through these means, cyberspace is portrayed as an infrastructure made up of technical hardware components. This framing removes other concerns, such as ethical or political,

---

[120] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Public Law 107–56, 107th Congress, October 26, 2001. Sect 1016e.
[121] *The National Strategy to Secure Cyberspace,* 6

from the discussion of cyberspace and instead focuses on technical. Through this single lens, it is implied that cyberspace is technical and therefore reserved for experts alone.

In *The National Strategy to Secure Cyberspace*, cyberspace is categorized as both a referent object and a threat. Ultimately, this has the effect of strengthening the securitization. As a threat to critical infrastructures, actions can be taken against cyberspace in the name of protecting other referent objects, like the economy, power grid, etc. By presenting cyberspace as a critical infrastructure itself, it makes it into a referent object. This allows action to be taken for the sake of protecting cyberspace itself, even when it does not pose a 'threat' to other referent objects. However, as both a threat and a referent object, cyberspace is presented as technical. However, cyberspace is not as technical as *The National Strategy to Secure Cyberspace* presents it to be.

Technification

Although *The National Strategy to Secure Cyberspace* characterizes cyberspace as both a threat and an infrastructure, it offers an incomplete picture of cyberspace. These characterizations falsely display cyberspace as an entirely technical realm. However, this is not the case. In her book *Cyberpolitics in International Relations,* Nazli Choucri defines cyberspace as

> a hierarchical contingent system composed of (1) the physical foundations and infrastructures that enable the cyber playing field, (2) the logical building blocks that support the physical platform and enable services, (3) the information content stored, transmitted, or transformed, and (4) the actors, entities and users with various interest who participate in this arena in various roles.[122]

Choucri's presentation of cyberspace is meant to be very comprehensive. Choucri defines cyberspace as more than merely technical components. Instead, Choucri presents

[122] Choucri, 8

cyberspace as a four-layer model. At its base, cyberspace is infrastructure, made up of physical components. These are the components that *The National Strategy to Secure Cyberspace* refers to when exhibiting cyberspace as a referent object. Built upon this base level of infrastructure are logical building blocks that support the structure of cyberspace. This layer can be thought of as the 'code' or protocols that give cyberspace its rules and structure for how it functions.[123] This is often the level referenced when *The National Strategy to Secure Cyberspace* criticizes vulnerabilities in cyberspace's design. Thus, both layers are part of the securitization- presented as the threat or object that needs protection. However, these are only two of the levels. After the infrastructure and logical building blocks is the actual information and content in cyberspace itself that makes up interactions. Finally, at the top layer of this model are the end users themselves. Through this understanding, cyberspace is more than merely technical components. Rather, cyberspace includes information and content, like websites and emails, along with people who create and consume it. This in turn makes cyberspace political. Cyberspace affects human agency, despite frames that indicate it is technical. Thus, any decisions that make changes to cyberspace, even in the name of security, have impacts on the users who are human beings.

The National Strategy to Secure Cyberspace falsely gives the perception that cyberspace is merely technical. Moreover, *The National Strategy to Secure Cyberspace* falsely gives the appearance that because cyberspace is technical, it can be secured from malicious actors through technical means. This is implied throughout the report. After all,

---

[123] Klimburg, Alexander, and Philipp Mirtl. *Cyberspace and Governance—A Primer*. Austrian Institute of International Affairs. Institute for Security Studies Africa.

The National Strategy to Secure Cyberspace's purpose is "to engage and empower Americans to secure the portions of cyberspace that they own, operate, or control"[124] with the guidance of the report. Furthermore, *The National Strategy to Secure Cyberspace* continually offers the Department of Homeland Security and other governmental agencies as authorities to guide action in securing cyberspace. The report is confident in the ability of these organizations to secure cyberspace, writing "In the future, working with a computer, the Internet, or any other cyber system may become as dependable as turning on the lights or the water."[125] Through this characterization, technical expertise can be leveraged in order to secure cyberspace. Cyberspace is presented similarly to a utility, where presumably technical experts are the plumber or electrician. However, unlike these utilities, cyberspace does not deliver a commodity to the homes of the public, but instead brings unique and personalized content from human interaction from across the globe.

As Choucri demonstrates, cyberspace is not merely technical components such as technical infrastructure and mechanisms that make cyberspace work. Cyberspace includes the content of cyber interactions and the users who are interacting. However, this technification serves a purpose. According to Hansen and Nissenbaum,

> Technifications are, as securitizations, speech acts that ''do something'' rather than merely describe, and they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves. The mobilization of technification within a logic of securitization is thus one that allows for a particular constitution of epistemic authority and political legitimacy[126]

---

[124] *The National Strategy to Secure Cyberspace,* 1
[125] *The National Strategy to Secure Cyberspace,* 35
[126] Hansan and Nissanbaum, 1167

Technification constructs an issue as technical, making it unavailable to the public. In technification, the securitizing actors hold an elevated status over the public with expertise or knowledge of the issue. As experts, they are trusted to construct the issue using their expertise in order to allow it to be understood by the public. However, due to the fact that the issue is technical, the public perceives the expert's construction of the issue as politically neutral in the same way which technology is perceived to be neutral. Therefore, when experts securitize an issue, the experts are not seen as securitizing agents, rather they are seen as extensions of the technology over which they have expertise and their assessment is seen as neutral. However, as Choucri demonstrated through her characterization of cyberspace, it is not merely technical. Along with infrastructure and mechanisms, cyberspace includes the information content and actors in cyberspace. Thus, decisions regarding cyberspace are not merely technical, but are political. Decisions regarding the security of cyberspace have implications on the content and actors within cyberspace.

Technification played a big role in the securitization of cyberspace in *The National Strategy to Secure Cyberspace.* By portraying the threat that cyberspace presents to critical infrastructures as technical, threat comprehension is closed off to the public and reliant upon experts for understanding. Similarly, by portraying the threats facing cyberspace as a critical infrastructures as technical, comprehension of threats facing cyberspace is also closed off to the public and reliant upon experts for understanding. Regardless of whether cyberspace is being characterized as a threat or an object that is threatened, in both cases the danger is described as technical. This closes off discourse about the danger to the public, because without experts describing the technical

threat, the public cannot understand the danger it presents. As a result, when threats are presented as technical, experts are relied upon to construct the threat for the public. However, this has consequences.

For instance, *The National Strategy to Secure Cyberspace* blames 'mechanisms of the Internet' for creating vulnerabilities in cyberspace that then threaten critical infrastructures. Many accept this as a black and white assessment in the same manner they would if a car mechanic said air leak was threatening tire pressure. In fact, a Gallup poll from February 2016 found that 73% of Americans believe cyber terrorism[127] will be a critical threat to vital US interests over the next ten years.[128] Clearly, the public is not only aware of the threats in cyberspace but also they accept the notion that these cyber threats are a danger to US national security. Furthermore, polls suggest that these perceptions have been growing over time. Prior to the February poll, Gallup had not asked about cyber terrorism as a future threat facing the United States. However, previous Gallup polls did find that people worried about cyber security in terms of crime. A 2014 Gallup poll found that 69% of Americans worried about computer hackers stealing their credit card information and 62% worried about having a smartphone or computer hacked.[129] While these polls do not show that Americans accepted cyber security in terms of national security, they do demonstrate that the public feared cyber threats could endangered their well being. Furthermore, these polls show that other

---

[127] Gallup defines cyber terrorism as "the use of computers to cause disruption or fear in society." In the study, only two threats polled higher than cyber terrorism: International Terrorism (79%), and the Development of nuclear weapons in Iran (75%).
[128] McCarthy, Justin. "Americans Cite Cyberterrorism Among Top Three Threats to U.S." Gallup.com.
[129] Riffkin, Rebecca. "Hacking Tops List of Crimes Americans Worry About Most." Gallup.com.

narratives regarding cyber security could frame threats in terms of crime instead of national security. In 2013 CBS News et. al found that nearly 57% of Americans labeled cyber attacks to computer systems as a 'very serious' threat in the United States.[130] Thus, acceptance of expert assessments of cyber security appears to be increasing amongst the public.

Although the public accepts these experts' assessments of cyber security and their description of threat, the assessments themselves are not black and white but instead exist in shades of gray. Expert assessment of threat in cyberspace is not inherently neutral. Rather, technification

> constructs the technical as a domain requiring an expertise that the public (and most politicians) do not have and this in turn allows ''experts'' to become securitizing actors while distinguishing themselves from the ''politicking'' of politicians and other ''political'' actors.[131]

In addition to being thought of as extensions of the technologies over which they have expertise, experts are distinguished from political actors that may have political agendas. However, giving experts the ability to describe the threat on behalf of the public gives experts the ability to control the frame surrounding a security issue. Framing is an important concept to consider as it relates to the Copenhagen School and Securitization Theory more broadly. In her book *Frames of War: When is Life Grievable?*, Judith Butler explores how war is understood and framed under the collective influence of the state, the media, and the public through reporting. Through framing, these actors are "selectively

---

[130] CBS News, 60 Minutes, and Vanity Fair. *CBS News/60 Minutes/Vanity Fair National Survey, March #3, 2013.* Report. March 3, 2013., Q15

[131] Hansen and Nissenbaum, 1167

producing and enforcing what will count as reality."[132] By controlling the content of reality- actors have the power to create a reality that is beneficial for an agenda. Butler writes that this can be used to get the population behind their mission in times of war, even when this mission ensures violence. For example, war can be framed by the state as "an inevitability, something good, or even a source of moral satisfaction."[133] This framing is very powerful- and even allows the state to "constitute and de-constitute personhood within the field of war."[134] Personhood can be associated or disassociated for the benefit of war waging. Population of opposing sides is not seen as persons, but instruments of the other side's capability for violence. Thus, attacking opposing population is not an act of violence against persons, but an attack against the instruments of violence in the opponent. While Securitization theory does not draw upon Butler's understanding of framing, framing can be used to securitize. Framing gives those who report to the public (in Butler's book it is reporters, but in this thesis it is technical experts) the ability to control what does and does not constitute reality by controlling what they do or do not include in their description or report.

As Butler demonstrates, framing is very powerful. Reality is presented and understood in how it is constructed or framed. By giving technical experts the power to frame issues of security in cyberspace, they are given the power to create the reality through which the threat is understood. This is also the reality on which decisions are based when it comes to taking action in response to threats. Yet, through technification, these realities are accepted as neutral and apolitical. However, the power to frame in fact

---

[132] Butler, Judith. 2009. *Frames of War: When Is Life Grievable?* London: Verso, 2009., xiii.
[133] Ibid., ix.
[134] Ibid., xii.

is very political because it informs decisions and desires when it comes to taking action in the name of security. Ultimately, by framing a threat as urgent, it warrants exceptional action in response. Thus, as Butler demonstrates, framing can be used to justify exceptional action by the state, including violence. A particular frame also excludes other ways in which the issue or actor can be understood—it excludes other possible frames.

Ultimately, *The National Strategy to Secure Cyberspace* does not provide the state with extraordinary powers in cyberspace. Additionally, the report does not call for any extraordinary actions. This is in part because the report was not meant to be a binding law; rather it was intended to be a collaborative strategy built as a public private partnership. However, what *The National Strategy to Secure Cyberspace* does do is frame cyberspace in terms of national security. Additionally, it demonstrates the US government beginning to take an active role in securing cyberspace. As a truly global network, tension exists between state power and governance and security in cyberspace. The state does not necessarily have the power to 'secure' cyberspace because it does not necessarily fall into a single jurisdiction. Recognizing this point, the report makes recommendations, but any mandates or requirements were removed from initial drafts. Many critics complained that as a result of this, the report "simply 'addresses' various security 'issues' instead of directing the 'resolution' of security problems."[135] However, what *The National Strategy to Secure Cyberspace* does succeed at is strengthening the process of securitization of cyberspace through technification.

The National Strategy to Secure Cyberspace demonstrates efforts by the state to exercise some level of control in cyberspace by framing issues of security within

---

[135] Zimmer, Michael. "The Tensions of Securing Cyberspace: The Internet, State Power & the National Strategy to Secure Cyberspace." *First Monday* 9, no. 3 (March 2004).

cyberspace. Ultimately, controlling this frame gives the power to control the reality through which cyberspace is understood. To these ends, *The National Strategy to Secure Cyberspace* frames issues of cyberspace as technical. Through the technical frame, issues of security in cyberspace are unavailable to the general public. This allows the government to act in order to manage the technical threat. Furthermore, the threat can then be framed with a desired action or outcome in mind. This in turn gives the government some level of control in cyberspace. This is one of the key implications of this securitization process and will be further discussed, along with other sociopolitical implications, in the Conclusion.

Conclusion

Through analysis of the both "The Report on the President's Commission on Critical Infrastructure Protection" in 1997 and *The National Strategy to Secure Cyberspace* in 2003, as well as an explanation of the historical context surrounding them, this thesis demonstrates how cyberspace became securitized. Cyberspace became conceived of as a realm that was uniquely technical. Consequentially, technical experts were given the authority to constitute security for cyber vulnerabilities in roles that were traditionally held by foreign policy or national security advisors. Initially, cyber security was characterized primarily in terms of risk, which could be managed through technical expertise. However, after September 11th vulnerabilities in cyberspace became characterized as active threats. In response to these threats, organizations like the Department of Homeland Security would act to secure cyberspace from the threat of terrorism. Within this effort, technical experts acted as securitizing agents, securitizing cyberspace through technification.

In addition to securitizing cyberspace, technification gives experts the ability to frame threats in cyberspace. These experts constitute technical threats as existing in cyberspace on behalf of the public. Often their assessment is accepted as neutral, just as technologies are accepted as neutral. However, the ability to assess gives these experts the power to frame threats in cyberspace, which is political. Framing creates the reality through which the public to understand the threats in cyberspace. Furthermore, this framing is used to determine the appropriate action to take against threat. In cyberspace, this framing has been used by many to advocate for changes in the structure of the

Internet. While these changes are advocated in the name of security, ultimately they exist within a broader tension between the Internet and the nation-state over state power.

Robert Khan, the creator of the TCP/IP protocols that created the Internet by allowing inter-networking, promoted four principles for transmission protocols between networks. Khan opted for a decentralized design and open architecture that would create 'gateways' between networks relying on a common language or protocol.[136] He used the principles below as the basis for transmission protocols for the inter-network:

- Each distinct network should have to stand on its own, and no internal changes should be required to any such network to connect it to the Internet.
- Communications should be on a best-effort basis. If a packet didn't make it to the final destination, it should be retransmitted shortly from the source.
- Black boxes would be used to connect the networks; these would later be called gateways and routers. There should be no information retained by the gateways about the individual packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery from various failure modes.
- There should be no global control at the operations level.[137]

These principles were chosen because they would make internetworking easy to adopt, which in turn would promote participation in the Internet. However, these principles, which would become the basis for the design of the Internet, put pressure on the state within its national security efforts. Due to principles that make up the Internet's design, "the Internet lacks any loci of control from which to monitor and/or block potentially harmful actions."[138] No global control exists over the Internet due to its decentralized design. Consequentially, this prevents a state from having a central point from which they can oversee or control the Internet's traffic. The design therefore poses an obstacle to

---

[136] Bidgoli, Hossein. *The Internet Encyclopedia, Volume 2*. 2nd ed. Hoboken: John Wiley & Sons, 2003., 119.
[137] Clarke, Richard A., and Robert K. Knake. Cyber War: The next Threat to National Security and What to Do about It. New York: Ecco, 2010., 43.
[138] Zimmer, Michael. "The Tensions of Securing Cyberspace: The Internet, State Power & the National Strategy to Secure Cyberspace." *First Monday* 9, no. 3 (March 2004).

states as they seek to identify and prevent threats in cyberspace. Additionally, the Internet is "indiscriminate as to its content,"[139] sending the contents of packets end to end on a best-effort basis. The Internet as a system is unaware of the content it is sending, meaning it cannot distinguish whether content is normal and harmless, or sensitive/ malicious. This further complicates states' national security objectives by making it nearly impossible to identify packets of content as threats while they pass through networks.

As a result of these complications, many, including PCIPB Chairman Richard Clarke, have argued that Khan's principles for the Internet's design created the basis for security problems.[140] This is evident throughout *The National Strategy to Secure Cyberspace*, which criticizes the mechanisms of the Internet for creating vulnerabilities. However, some have taken the criticisms a step further and advocated for changes in design of the Internet due to concerns about the security resulting from these principles. For instance, former Director of National Intelligence Mike McConnell said in a 2010 interview with *The Washington Post*,

> We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options—and we must be able. More specifically, we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment—who did it, from where, why and what was the result—more manageable[141]

Although McConnell proposes a technical change to the Internet, the outcome of his proposal is political. McConnell's proposed reengineering of the Internet would make states' process of determining threats in cyberspace more manageable by allowing things

---

[139] Zimmer, Michael. "The Tensions of Securing Cyberspace: The Internet, State Power & the National Strategy to Secure Cyberspace." *First Monday* 9, no. 3 (March 2004).
[140] Clarke., 43.
[141] Rid, Thomas. 2013. *Cyber war will not take place*. Oxford; New York: Oxford University Press.,139-140

like location and attribution to be more easily credited. However, these changes would give the state the power to govern and secure the Internet, a global network that extends far beyond its borders, in the name of national security. While these changes have not been made, technification gives government organizations of technical experts the ability to advocate for technical changes to cyberspace in the name of security. While these changes are technical, their implications are political as the stakes are control over the governance of the Internet and a new answer to the long-standing question about the extent of a role that the state should play in governance over a global network.

This thesis primarily focused on the securitization of cyberspace through technification by examining the history and themes within "The Report of the President's Commission on Critical Infrastructure Protection" and *The National Strategy to Secure Cyberspace.* Beyond this thesis, future research could be done to examine technification and the threat assessment process in cyberspace within the organizations such as the Department. of Homeland Security. Furthermore, additional research could build on this argument about the securitization of cyberspace and look at militarization in cyberspace through the creation of bodies like Cyber Command. Finally, more research could be done to examine what may have occurred if the securitization of cyberspace had not been successful or if the public suddenly stopped accepting the narrative that cyberspace is both a source of threats and also a vulnerable to external attacks. This would alter the understanding of cyberspace, allowing it to become less associated with threat and security; which in turn would affect ongoing debates, such as those occurring over encryption between the FBI and Apple. More research could therefore examine how these debates would change if cyberspace were not contextualized in terms of security.

Acknowledgements

I would first like to thank my thesis committee chair Dr. Priya Dixit. Dr. Dixit dedicated much of her time reviewing drafts, giving edits/feedback, and providing guidance since the beginning of the thesis process. I would also like to thank my other committee members, Dr. Paul Avey and Dr. Scott Nelson, as well for their time and feedback on this project.

I also wanted to acknowledge Patrick Deegan, Daniel Cotter, Brianna Hamadé, and all of my fellow graduate students in the Political Science program. I am thankful for their support and encouragement along the way that kept me going.

Finally, I would like to thank my parents, Karl and Linda Schwarz. I cannot begin to express how profoundly grateful I am that they provided me the opportunity to pursue an education at Virginia Tech. This accomplishment would not have been possible without them.

Kevin Schwarz

Bibliography

Amoore, Louise. Politics of Possibility : Risk and Security Beyond Probability. Durham: Duke University Press, 2013.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: Sage., 21.

Bennett, Amy. "UPDATE: US Drafts National Strategy to Secure Cyberspace." ITworld. September 18, 2002. Accessed March 18, 2016. http://www.itworld.com/article/2806338/business/update--us-drafts-national-strategy-to-secure-cyberspace.html.

Bidgoli, Hossein. *The Internet Encyclopedia, Volume 2*. 2nd ed. Hoboken: John Wiley & Sons, 2003.

Butler, Judith. 2009. *Frames of War: When Is Life Grievable?* London: Verso, 2009.

Buzan, Barry, and Ole Ver. *Security: A New Framework for Analysis*. Boulder, Colo.: Lynne Rienner Pub., 1998

CBS News, 60 Minutes, and Vanity Fair. *CBS News/60 Minutes/Vanity Fair National Survey, March #3, 2013.* Report. March 3, 2013. http://doi.org/10.3886/ICPSR34998.v.

Center for Strategic and International Studies. June 2014. Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II

Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, Mass.: MIT Press, 2012

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

Clinton Administration, Presidential Decision Directive 63 (PDD-63): Policy on Critical Infrastructure Protection (May 22, 1998)

Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997.

Executive Order 13228 of October 8, 2001, Establishing the Office of Homeland Security and the Homeland Security Council. Code of Federal Regulations, title 3 (2001): 51812 - 51817

Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age. Code of Federal Regulations, title 3 (2001): 53063 -53071

Giddens, Anthony. 1999. "Risk and Responsibility". *The Modern Law Review* 62 (1). Wiley: 1–10.

Girvan, Norman. 2010. technification, sweetification, treatyfication. *Interventions* 12 (1): 100-11.

Hansen, Lene, and Helen Nissenbaum. 2009. Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly* 53 (4): 1155-1175.

Hjalmarsson, Ola. "How the Web Was Won." Master's thesis, Lund University, 2013. http://lup.lub.lu.se/student-papers/record/3357990.

Klimburg, Alexander, and Philipp Mirtl. *Cyberspace and Governance—A Primer*. Austrian Institute of International Affairs. Institute for Security Studies Africa. September 2011. https://www.issafrica.org/acpst/uploads/Klimburg_Cyberspace_and_Governance-A_primer.pdf.

Kremer, Jan, and Benedikt Müller, eds. *Cyberspace and International Relations: Theory, Prospects and Challenges*. Springer, 2014.,

Lawson, Sean. "With Drone Strike On ISIS Hacker U.S. Escalates Its Response To Cyber Attacks."*Forbes*, September 12, 2015.

Lindsay, JR. 2013. Stuxnet and the limits of cyber warfare. *Security Studies* 22 (3):

Magnan, Stephen W. "Safeguarding Information Operations: Are We Our Own Worst Enemy." Central Intelligence Agency. June 27, 2008. Accessed March 12, 2016. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publicatfions/csi-studies/studies/summer00/art08.html.

Mcgraw, Gary. "Cyber War Is Inevitable (Unless We Build Security In)."*Journal of Strategic Studies* 36, no. 1 (2013): 109-19.

McCarthy, Justin. "Americans Cite Cyberterrorism Among Top Three Threats to U.S." Gallup.com. February 10, 2016. Accessed February 18, 2016. http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx.

Morgenthau, Hans J., and Kenneth W. Thompson. 1985. *Politics among nations: The struggle for power and peace*. 6th ed. New York: McGraw-Hill.

The National Strategy for Homeland Security. Washington, D.C.?: Office of Homeland Security, 2002.,

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Washington, D.C.: Dept. of Homeland Security, 2003.

The National Strategy to Secure Cyberspace. Washington, D.C.: Dept. of Homeland Security, 2003.

Nissenbaum, H. 2005. Where Computer Security Meets National Security. *Ethics and Information Technology* 7 (2). 61-73.

Pike, John. "Military: Eligible Receiver." Global Security. May 7, 2011. Accessed February 18, 2016. http://www.globalsecurity.org/military/ops/eligible-receiver.htm.

President's Critical Infrastructure Protection Board, Executive Office Of the President, The White House. “Notice of pending request for public comment regarding the National Strategy to Secure Cyberspace for comment”. Federal Register, Vol. 67, No. 201, October 17, 2002. https://www.gpo.gov/fdsys/pkg/FR-2002-10-17/html/02-26456.htm

Rid, Thomas. 2013. *Cyber war will not take place*. Oxford; New York: Oxford University Press

Riffkin, Rebecca. "Hacking Tops List of Crimes Americans Worry About Most." Gallup.com. http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx

Saad, Lydia. "In U.S., 11% of Households Report Computer Crimes, a New High." Gallup.com. http://www.gallup.com/poll/145205/new-high-households-report-computer-crimes.aspx

Stone, John. 2013. Cyber war will take place. *The Journal of Strategic Studies*36 (1): 101-8.

Sun, Helen. 2010. *Internet Policy in China: A Field Study of Internet Cafés*. Lanham, Md.: Lexington Books

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Public Law 107–56, 107th Congress, October 26, 2001.

Waltz, Kenneth N. 1962. *Man, the state, and war: A theoretical analysis*. New York: Columbia University Press.

Waltz, Kenneth N. 1979. *Theory of international politics*. Reading, Mass: Addison-Wesley Pub. Co.

Warren, Peter. "Hunt for Russia's Web Criminals." *The Guardian*, November 7, 2007, Technology sec.

White House. 2011. *INTERNATIONAL STRATEGY FOR CYBERSPACE Prosperity, Security, And Openness In A Networked World*.