2021

Deterrence and Response Improvements for a Large-Scale Cyberterrorism Attack

Harrison Cunningham
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Harrison E. Cunningham

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Glenn Starks, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Christopher Jones, Committee Member,
Public Policy and Administration Faculty

Dr. Joshua Ozymy, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Deterrence and Response Improvements for a Large-Scale Cyberterrorism Attack

by

Harrison E. Cunningham

MS, Troy University, 2014

MA, The University of Oklahoma, 2011

BA, Boston University, 2006

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2021

Abstract

A successful large-scale cyberterrorism attack has never been conducted against the United States, yet cyberterrorism is a real and evolving threat. The United States assumes a largely defensive posture toward the thousands of daily cyberattacks conducted against the country, allowing cyberterrorists to probe and execute cyberattacks with broad impunity. The United States would most likely respond to a successful large-scale cyberterrorism attack within a framework of regulations concerning physical acts of terrorism since no policy exists on how to respond to major cyberterrorism attacks. The purpose of this qualitative study was to explore the perceptions of U.S. terrorism and cybersecurity experts to understand how the country might better prevent, cope with, and respond to a large-scale cyberterrorism attack. Punctuated equilibrium theory provided a lens to understand the relationship between policy information flow and politically driven change to guide this study. Data were generated through one-on-one semistructured telephone interviews from nine cybersecurity and terrorism experts. These data were then coded and analyzed to interpret patterns and generate themes. Results indicated that the United States should not consider specific large-scale cyberterrorism attack response options since terrorists likely do not yet possess the capabilities to carry out a cyberattack. However, the country could do much more to prevent destructive cyberattacks, to include eventual cyberterrorism attacks, through deterrence. The implications for positive social change include improving the collective national cyber defense, from small private companies to large government organizations. This study can also raise U.S. policymaker cyberterrorism awareness through more extensive education and improved synthesis of cyber related information to support accurate determinations.

Deterrence and Response Improvements for a Large-Scale Cyberterrorism Attack

by

Harrison E. Cunningham

MS, Troy University, 2014

MA, The University of Oklahoma, 2011

BA, Boston University, 2006

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2021

Acknowledgements

Many thanks to my committee chair, Dr. Glenn Starks, for instilling in me the confidence to pursue this dissertation with a purpose. Also, thanks to Dr. Christopher Jones for the perpetual encouragement and impeccable advice from the beginning. Lastly, thank you to Dr. Joshua Ozymy for compelling me to reevaluate aspects of this dissertation to make it a much better final product.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

The United States acted quickly and aggressively following the terrorist attacks of September 11, 2001. The first retaliatory strikes in Afghanistan by the United States military occurred less than a month after 9/11 (Jenkins & Godges, 2011). Hundreds of U.S. Special Forces soldiers, Central Intelligence Agency operatives, and thousands of Northern Alliance tribesmen significantly weakened the Taliban regime and eliminated al Qaeda's safe haven by mid-December of that year (Hellmuth, 2018a; Jenkins & Godges, 2011). Nevertheless, counterterrorism operations in Afghanistan have been ongoing for 19 continuous years as of 2020, making the conflict the longest in U.S. history. The United States public has yet to lose support for this conflict to levels seen during the Vietnam War. However, an equally strong and sustained U.S. retaliatory offensive following a major cyberterrorism attack against the country might not be as well received, since already elusive terrorism guidelines would be further complicated with the inclusion of cyberterrorism.

A growing reliance on the cyber domain in recent decades has created a new opportunity for individuals and groups to infiltrate U.S. targets that would otherwise be unattainable (Neely & Allen, 2018). Government organizations at all levels, financial institutions, and defense agencies now maintain large networked digital databases full of sensitive information (Holt & Kilger, 2012). Additionally, the proliferation of automated systems integrated in U.S. critical infrastructure such as water, sewer, telephone, and power systems leaves them all vulnerable to cyberattacks (Klein, 2015).

Given the limited publicly available U.S. government guidance for major cyberterrorism attacks, I explored the perceptions of U.S. terrorism and cybersecurity experts to understand how the country might better prevent and respond to large-scale cyberterrorism attacks. A response prepared during the sensitive and fervent days and weeks following a successful large-scale cyberterrorism attack might not result in a plan as well-crafted as one preemptively modeled. Additionally, post hoc cyberterrorism regulations have the potential to be emotionally charged, which was the atmosphere that the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT, hereafter Patriot) Act was created in following 9/11.

Justifications for military conflict have been well documented throughout history. Past wars and the rationale for each have largely been rooted in the theory of realism which was first debated by the Ancient Greek historian Thucydides and has subsequently seen numerous evolutions over the last 2,500 years (Morkevičius, 2015). However, a realist viewpoint focuses on countries with respect to the international arena and therefore does not offer much information regarding terrorism (Morkevičius, 2015). Additionally, Islamic terrorism is sometimes considered merely a tactic or fad that will eventually fade within the international world order dominated by sovereign states (hereafter states) and can thus be downplayed by international relations scholars.

Though incomplete, justifications for the use of military force against terrorist organizations, such as the United States versus the Taliban and al Qaeda, still generally demand a humanitarian approach to warfare, or *jus in bello*. Yet, like realism, just war theory also has limited applications for counterterrorism operations (Taylor, 2017). This theory prescribes that the United States should fight terrorist organizations in a moral manner within the constraints of the country's constitutional democracy (Walzer, 2007). To further complicate matters, there is not one domestic or international agreed upon definition of terrorism despite extensive information being written on the subject (Dinniss, 2018; Gaibulloev et al., 2017; Marsili, 2019).

The United States classifies terrorists as *unlawful enemy combatants* as outlined in the Military Commissions Act of 2006 and in the Act's 2009 amendment (Goode, 2015). Unlawful enemy combatant is a classification that is internationally disputed since the Third Geneva Convention only delineates between prisoners of war and noncombatants (Goode, 2015). Because of this, the United States would have considerable difficulty justifying military retaliation against the perpetrators of a successful large-scale cyberterrorism attack considered unlawful enemy combatants residing in a country not in open conflict with the United States (Goode, 2015).

Cyberterrorism is a frequently debated subject with some scholars even suggesting that cyberterrorism should not be discussed separately from acts of physical terrorism (Jarvis & Macdonald, 2015). However, the largely accepted definition of cyberterrorism that I used for this study is: terrorism in cyberspace that features attacks against computers and networks by subnational groups or individuals through violence or fear to coerce or intimidate a state's government or citizens to further political or social objectives (Jenkins & Godges, 2011; Klein, 2015; Marsili, 2019; Warf & Fekete, 2016). Even though no large-scale cyberterrorism attack has been successful against the United

States, damaging attacks are still conceivable as the world becomes more dependent on technology and terrorists continue to look for new ways to pursue cyber vulnerabilities to achieve objectives (Albahar, 2019; Dinniss, 2018; Warf & Fekete, 2016). Consequently, scholars and military commanders alike are well aware of the threats posed by cyberterrorism and regularly discuss the probability of a successful cyberterrorism attack disrupting or destroying critical aspects of the U.S. military, financial, and service sectors (Neely & Allen, 2018; Wirtz, 2017).

This opening chapter includes an overview of the study. Chapter 1 is organized starting with the background, problem statement, and purpose of the study. These areas provide a foundation for the study by outlining conflict as it relates to cyberterrorism and the potential issues that could arise from conflict. The chapter then continues into the study's core and includes the research question, a brief description of the conceptual framework, and nature of the selected research paradigm and design. Next, definitions of key terminologies are provided along with illustrating study scope factors including limitations and delimitations. The chapter concludes with a statement of significance on why the study should be conducted before summarizing and transitioning to Chapter 2.

Background of the Study

No country has threatened victory over the U.S. military through conflict in decades. The United States has enjoyed complete military superiority in a unipolar world created after the fall of the Soviet Union in 1990. However, adversaries of the United States are constantly looking for ways to disrupt and defeat elements of the country through asymmetric warfare (Warf & Fekete, 2016).

As technology continues to exponentially increase in importance and sophistication, adversaries are finding ways to leverage these advancements for malicious intent. The United States would likely have *casus belli*, or justification for war, if a foreign government launched a cyberattack designed to cause catastrophic damage within the United States. However, if a foreign government covertly conscripted individuals or subnational organizations to carry out such an attack, the attack would be considered cyberterrorism. The lists of potential targets for cyberterrorists in the United States are vast (Albahar, 2019). The sheer number of targets essentially guarantees that terrorists will be able to exploit many exposed weaknesses (Klein, 2015). Whether state-sponsored or homegrown, cyberterrorism lets terrorists strike from virtually anywhere in the world making the attacks more sudden and less predictable (Albahar, 2019).

Hacking of U.S. agencies and businesses has been conducted by states, individuals, and groups driven by a wide range of motivations including profit, notoriety, and ideology. China has acknowledged the existence of the People's Liberation Army Unit 61398, which was created specifically for cyber activities (Warf & Fekete, 2016). In 2015 the United States accused Unit 61398 of stealing data from 141 U.S. businesses (Mazanec, 2016). Similarly, the military of the Democratic People's Republic of Korea (North Korea) has an elite hacking team known as Lab 110 modeled after, and possibly even trained by, Unit 61398 (Warf & Fekete, 2016). Lab 110 has successfully attacked U.S. Treasury Department servers on multiple occasions from 2009 to 2013 (Warf & Fekete, 2016). Lastly, Russia's Federal Security Service (FSB) has an extensive history of conducting cyberattacks and has even been accused of starting *Web War I* against

Estonia in April 2007, which prompted the Western world to begin discussing the reality of a cyberwar (Warf & Fekete, 2016). In addition to Estonia, the FSB has also been blamed for conducting cyberattacks against Georgia in 2008 and Ukraine in 2014 (Warf & Fekete, 2016). However, to date no cyberattacks designed to cause extensive damage within the United States have been successful (Klein, 2015; Kosseff, 2018).

The first and only successful cyberterrorism attack against the United States that has been brought to trial was conducted in 2015 by a Kosovo citizen named Ardit Ferizi, though the attack did not cause the deaths of any U.S. citizens as was its intent (Office of Public Affairs, 2016). In June 2015 Ferizi hacked into the server of a private U.S. company and extracted personally identifiable information on approximately 1,300 military and government employees (Office of Public Affairs, 2016). He then sent the information to Junaid Hussain, a member of the Islamic State of Iraq and Syria (ISIS), who published the information as a hit list on a website run by the Islamic State Hacking Division (ISHD; Office of Public Affairs, 2016). Ferizi was subsequently extradited from Malaysia to the United States where, in September 2016 he was sentenced to 20 years in prison for both providing material support to ISIS and gaining access to a protected computer without authorization (Office of Public Affairs, 2016). The Ferizi data dump was notable because it resulted in the only person in the United States convicted of cyberterrorism related charges as of 2020. However, Ferizi’s list was not the first or only United States related sensitive data release published by ISIS affiliated hacking organizations.

The ISHD first published a list of 100 U.S. military personnel in early 2015 prior to Ferizi's own list being released in August of that year (Nance & Sampson, 2017). A second list of 100 different U.S. military personnel was also released in September 2015 by ISHD following Ferizi's release (Nance & Sampson, 2017). Most recently, in May 2016 ISHD publicized the names and addresses of 76 United States military drone operators (Nance & Sampson, 2017).

Another ISIS affiliated hacking organization, the Cyber Caliphate Army, famously hacked the U.S. Central Command's YouTube and Twitter sites in January 2015 and released their own lists of U.S. military personnel on three separate occasions in December 2015 and in January 2016 which totaled over 200 names (Nance & Sampson, 2017). Finally, in April 2016 yet another ISIS affiliated hacking group, the United Cyber Caliphate, released the names of 3,600 New York citizens under the title, *We Want Them Dead* followed by three large data dumps in April and June 2016 that totaled over 22,000 U.S. citizens listed as *Revenge for Muslims* (Nance & Sampson, 2017).

Yet, dangerous cyberterrorism events continue to be overlooked by U.S. policymakers given the lack of resulting tangible physical harm (Warf & Fekete, 2016). As cyberterrorism events are ignored, so are the potential responses and justifications to those responses. However, cyberterrorism is a very real option for terrorists due to its anonymity, debilitating potential, and psychological impact. It could be in the interest of the United States to not only be prepared for a cyberterrorism attack but to also be ready with the country's response options following a successful attack. In this study, I addressed an existing gap in knowledge by considering better prevention and response strategies for a large-scale cyberterrorism attack against the United States.

Problem Statement

The United States assumes a largely defensive posture toward the thousands of daily cyberattacks conducted against the country. Cyberterrorists can therefore probe and execute cyberattacks against a host of U.S. networks with broad impunity. The United States would most likely respond to a successful large-scale cyberterrorism attack within a framework of regulations concerning physical acts of terrorism since no policy exists on how to respond to major cyberterrorism attacks against the country (Warf & Fekete, 2016). It is still legally unclear what attacks can even be considered cyberterrorism (Dinniss, 2018; Marsili, 2019; Warf & Fekete, 2016). Given the debilitating nature of cyberattacks and the potential to set off large-scale conflicts, the United States government may need to publish cyberterrorism prevention and response guidelines to better deter cyberterrorism attacks and dictate proportional response options. Policies aggressively preventing and condoning such attacks as well as articulating approved responses may result in countries being far less willing to sponsor destructive cyberterrorism attacks against the United States.

It is not known what terrorism and cybersecurity experts believe is the best way to prevent and respond to large-scale cyberterrorism attacks against the United States. A need therefore exists to learn more about U.S. cyberterrorism guidelines from the perception of experts. This research fills a gap in literature by presenting expert analysis on current U.S. government cyberterrorism policy including the validity of creating or improving U.S. cyberterrorism deterrence and response guidelines.

Purpose of the Study

The purpose of this qualitative study was to explore the perceptions of terrorism and cybersecurity experts in the United States to better understand how the country might prevent and respond to large-scale cyberterrorism attacks. A major successful cyberterrorism attack has never been conducted against the United States so it remains unseen what guidelines the country will use as the basis for a response. The current lack of guidance could leave the United States in a vulnerable position following a successful large-scale cyberterrorism attack given the unpredictability of potential responses. Through expert interviews, the study addressed if additional measures may be needed to better handle aspects of major cyberterrorism attacks, or if current policies are adequate to respond to these attacks.

Research Question

Research Question: How do terrorism and cybersecurity experts perceive that the United States might better prevent, cope with, and respond to large-scale cyberterrorism attacks?

Conceptual Framework

I used punctuated equilibrium theory to analyze the prospect of creating specific cyberterrorism response guidelines for the U.S. government. Punctuated equilibrium theory was introduced by Frank Baumgartner and Bryan Jones in *Agendas and Instability in American Politics* in 1993 (Baumgartner et al., 2018). This theory was designed to be broadly applied to a range of policymaking initiatives and focuses on policy change driven by political organizations during protracted periods of stability coupled with bouts of immediate change (Koski & Workman, 2018). Punctuated equilibrium theory has been used to address budget change and health initiatives as well as policies covering environmental, energy, tobacco, education, and political topics (Flink, 2017; Kuhlmann & Van der Heijden, 2018).

The political process is both rapid and slow as policymakers implement existing policies or create new ones to adapt to new information and changing needs (Baumgartner et al., 2018; Flink, 2017). Punctuated equilibrium theory suggests that governments often receive an overabundance of information that overloads individual cognitive processing abilities (Koski & Workman, 2018; Kuhlmann & van der Heijden, 2018). Information is therefore not accurately synthesized, which results in some policy issues being initially ignored with the potential for future overcorrections (Flink, 2017; Koski & Workman, 2018). For example, overinformed and overtasked policymakers have been displacing U.S. terrorism policy into a subsidiary role in favor of agendas that have the potential for explosive change such as COVID-19 economy stabilization, political reorganizing following the November 2020 presidential election, and new Department of Defense guidance shifting military focus away from terrorism and toward near-peer adversaries.

Punctuated equilibrium theory shows that all policy systems are susceptible to policy change through error correction or error accumulation (Baumgartner et al., 2018; Koski & Workman, 2018). Policymaking is incremental in the realm of error correction since policy is constantly adjusted in response to new information. Yet, organizational responses are never quite proportional to the problem due to *disproportionate information processing*, which can lead to punctuated changes (Flink, 2017; Koski & Workman, 2018). In error accumulation, policy does not respond to negative information due to barriers in the policymaking process. In this situation, pressure builds until a drastic policy change is required (Flink, 2017; Koski & Workman, 2018). This study could help U.S. policymakers avoid cyberterrorism error accumulation by identifying barriers preventing the formation of improved U.S. cyberterrorism deterrence and response options while also capitalizing on incremental change during stasis. A more detailed description of punctuated equilibrium theory relating to this study is given in Chapter 2.

Nature of the Study

Rudestam and Newton (2015) explained that the goal of research is to link the theoretical level with the empirical level. This qualitative study addressed the perceptions of U.S. terrorism and cybersecurity experts in order to support an open-ended hypothesis. I used a systems approach for this qualitative study. Patton (2015) explained that a systems perspective is important in dealing with real world interconnections and viewing things as being imbedded in larger holes. He stated that a holistic mindset is central to a systems approach since the properties of a system are lost when taken apart, and that synthetic thinking should also be applied in which the whole is explained (Patton, 2015). Patton (2015) finally believed that systems thinking is perfect for analysis where the area as a whole is reviewed for strengths and weaknesses.

In this study, I addressed perceived appropriate deterrence and response options for cyberterrorism attacks based on expert interviews. These options are decided within the context of the government, which is the identified system in this study. Individual components of the system are various government agencies such as the executive branch and its components, the Department of Defense, and the Department of State. Each organization has different focuses on terrorism and cybercrimes and they all, therefore, have their own characterizations concerning cyberterrorism laws. There is not one standard definition of terrorism within the United States (Dinniss, 2018; Gaibulloev & Sandler, 2019; Hoffman, 2017; Marsili, 2019). Instead, each organization has created their own definition to suit their specific points of focus. Based on a systems approach, I addressed if current guidelines are enough to adequately deter and respond to a cyberterrorism attack, or if more robust guidelines should be considered.

I used a one-on-one semistructured telephone interview as the instrument for this study to allow leeway for script diversions for clarifications or to grasp deeper meanings to answers. I identified the participants in this study through demonstrated expertise in their respective terrorism and cybersecurity career fields as they relate to cyberterrorism. I lastly assumed that data saturation would occur between eight to twelve individuals.

Definitions

Bounded Rationality: This idea denotes that policymakers are limited by cognitive limitations (Baumgartner et al. 2018).

Critical Infrastrucure: Defined in the United States as systems relating to cyber and physical defense, the economy, and public safety and health whose destruction or incapacitation would have debilitating impacts on their related sectors (Haber & Zarsky, 2017).

Cybersecurity: A state's ability to guard cyberspace from crime, fraud, sabotage, espionage, and other destructive interactions using tools, policies, and actions (Weiss & Jankauskas, 2018).

Cyberspace: Computer and trancastional networks that store, send, and share information online as well as the physical computer systems and infrastructure that enable the flow of information and machine interaction (Klein, 2015; Weiss & Jankauskas, 2018).

Cyberterrorism: Terrorism in cyberspace that features attacks against computers and networks by subnational groups or individuals through violence or fear to coerce or intimidate a state's government or citizens to further political or social objectives (Jenkins & Godges, 2011; Klein, 2015; Marsili, 2019; Warf & Fekete, 2016).

Cyberwarfare: Malicious actions in cyberspace that result in outcomes comparable to major kinetic violence (Shad, 2018).

Disproportionate Information Processing: Processing that contributes to the rate of policy change associated with punctuated changes described in punctuated equilibrium theory (Flink, 2017).

Punctuated Equilibrium Theory: A policy process theory for understanding change in organizations. Punctuated equilibrium theory posits that political processes operate primarily in stable environments defined by measured progress (Baumgartner et al., 2018). Yet, these same enviroments can also experience significant political change

(Baumgartner et al., 2018). The cause of change is driven by political agendas and information flow and can be hindered by institutional friction or limited cognative abilities (Baumgartner et al., 2018; Flink, 2017; Kuhlmann & Van der Heijden, 2018).

Systems Approach: An approach dealing with real world interconnections as being imbedded in larger holes (Patton, 2015). A holistic mindset is therefore central to this approach since the properties of a system are lost when taken apart (Patton, 2015). The United States government was the system for this study.

Assumptions

Assumptions are aspects of the study that are believed but cannot be demonstrated to be true (Creswell, 2013). I assumed that all participants were knowledgeable on subjects related to their professions and that they all understood the context of the research. I chose the participants due to their notable resumes and accomplishments in their respective fields and I assumed that all participants provided accurate information. Lastly, I assumed that my military background as a member of the intelligence, surveillance, and reconnaissance community had no effect on the data collected and its public release.

I obtained all information used in this study from open source information. I had access to classified databases but did not utilize any government networks to search for cyber or terrorism specific information while enrolled in the doctoral program. I assumed, therefore, that the military public affairs office would promptly allow the release of this study.

Scope and Delimitations

United States cyberterrorism prevention and response strategies were the sole focus for this study, while excluding the applicability of creating specific laws related to a cyberterrorism attack. Since U.S. laws apply mainly to U.S. citizens, cyberterrorism laws would need to include a discussion on projecting laws into foreign countries as well as creating and amending international treaties to respond to cyberterrorism threats. Additionally, laws are more general in nature while a prevention and response narrative focuses on specific actions based on specific events determined by the residing national leadership. Because of this, an in-depth study of past laws concerning cybersecurity and terrorism were omitted and the research instead focused on a qualitative study using participant interviews to gain the perception of terrorism and cybersecurity experts.

This study could serve to promote dialogue between different federal government and private organizations under the common impetus of cyberterrorism. I gathered all information through interviews, allowing participants to focus on information they felt was relevant and important. Cyberterrorism is a new and evolving field, driving current information to become quickly outdated which is why the study relied heavily on expert knowledge.

Limitations

Limitations are potential weaknesses in a study that are out of the researcher's control (Creswell, 2013). The main limitation of this study was the potential for incomplete information due to a limited number of participants. Creswell (2013) recommended three to ten contributors, and Morse (1994) suggested six participants to understand the core of the topic. While Creswell (2013) and Moore (1994) offered firm numbers, Merriam (2009) believed sampling size depended on many factors including research questions and data collection. Finally, both Merriam (2009) and Patton (2015) identified resource limitations as a major factor for determining sampling size.

All study participants worked in various government, security, legislation, and educational sectors so the perceptions of their knowledge could have been skewed by their own lived experiences. Another major limitation of this study was not knowing what controlled or classified guidance exists within the many U.S. government layers for preventing and responding to cyberterrorism attacks. However, classified information concerning cyberterrorism could not be used for public policy formation given the secret nature of the information not made available to every policymaker or foreign government.

I strived for unbiased research throughout this study, yet as a new researcher, it was imperative for me to identify and attempt to mitigate all potential biases before beginning the research. Above all, I attempted to avoid conformation bias by not forming any premature hypothesis or beliefs concerning cyberterrorism. I also objectively collected and analyzed all information before drawing any conclusions.

Significance of the Study

In this study, I investigated if cyberterrorism policies could be improved to ensure that a future U.S. federal government response to a large-scale cyberterrorism attack is effective, is in line with the values of the United States, and is also palatable with the international community. A multitude of domestic policies are created to directly address acts of physical terrorism. These policies could also be used to prevent and persecute acts of cyberterrorism. However, it might not be ideal to utilize physical terrorism policies to guide U.S. cyberterrorism agendas given the inconclusive nature of cyberattacks as well as the many disconnects between U.S. and international guidelines.

The United States government has not given serious thought to a large-scale cyberterrorism attack partially because terrorists are still believed to lack the technology to conduct these destructive attacks (Fidler, 2016; Nance & Sampson, 2017). Further, no scholarly research has been drafted to advocate for cyberterrorism specific policies designed to prevent or respond to debilitating cyberterrorism attacks within the United States. The only U.S. regulation that directly addresses cyberterrorism is section 814 *Deterrence and Prevention of Cyberterrorism* of the non-permanent Patriot Act (Podgor, 2002). However, section 814 focuses on penalties for individuals gaining unauthorized access to computers which would not benefit the United States in the aftermath of a successful large-scale cyberterrorism attack.

Given this lack of guidance, the United States government has the potential to make mistakes while attempting to retaliate from a successful significant cyberterrorism attack in a timely manner against an elusive enemy. An aggressive unilateral response by the United States to a cyberterrorism attack could subsequently generate negative repercussions against the country domestically, as well as from the greater international community. Yet, the negative effects of a retaliation could be minimized if the United States preemptively implemented an all-inclusive and universally palatable cyberterrorism strategy.

Summary

Terrorism is an evolving definition which is often tailored to align with the purposes of federal government entities each offering their own specific descriptions. There are also no sanctioned categories for terrorists at the international level as is evidenced by the United States' controversial assertion of unlawful enemy combatants. The inclusion of cyber in the pursuit to define and categorize terrorists only serves to make the task of accurately classifying terrorists more complicated.

A vast majority of cyberattacks conducted against the United States have been thwarted, though cyberattacks attacks have and will continue to be successful against all levels of the U.S. government and industry. The country's ever-increasing reliance on technology provides more daily opportunities for cyberattacks to occur in places within the United States that were once deemed untouchable. Terrorists are currently assessed to not possess the technology to conduct a damaging cyberattack against the United States, but the threat is getting more tangible with each passing day. It could also be in the realm of possibilities for terrorists to surprise the world with a large-scale cyberterrorism attack within the United States just as they did conventionally on September 11, 2001.

The United States has strict rules in place that guide conventional responses to hostilities. Following a large-scale cyberterrorism attack against the country, the U.S. government could adapt these guidelines to suite a new type of warfare, or they could ignore them all together. Either way, decisions would be made with incomplete information by U.S. leaders in the tense aftermath of a successful large-scale cyberterrorism attack. Because of this, it might benefit the U.S. government to draft a succinct response plan to a large-scale cyberterrorism attack in order to be prepared to respond smarty to any such attack and to also highlight a deterrence plan in order to prevent cyberterrorism attacks from occurring at all.

In Chapter 2, I provide an exhaustive review of the current literature related to cyberwarfare, terrorism, and cyberterrorism and identify the databases used to obtain this literature. I also expand on punctuated equilibrium theory and relate it to previous cyberterrorism associated work. I lastly review and synthesize available literature as it relates to the research question in order to justify the holistic thinking based on a systems approach.

Chapter 2: Literature Review

Research Problem and Purpose

A successful large-scale cyberterrorism attack against the United States could have the potential to set off a widespread conventional military conflict. Because of this, the U.S. government may need to create a cyberterrorism specific plan to outline deterrence initiatives and draft proportional response options. Cyberterrorism prevention and response plans would serve to quickly and effectively bolster defenses or facilitate responses that are in line with all previously considered domestic and international guidelines and principles.

The purpose of this qualitative study was to explore the perceptions of terrorism and cybersecurity experts in the United States to better understand how the country might prevent and respond to large-scale cyberterrorism attacks. The U.S. government will act in an unpredictable manner following a successful large-scale cyberterrorism attack against the country because the attack would place the government in an unfamiliar position with limited guidance. Yet, no public U.S. research or legislation exists for prevention and response strategies related to a large-scale cyberterrorism attack. In this chapter, I give a detailed review of all publicly available information on cyberterrorism that I acquired using several approaches to ensure that all information was extracted.

Literature Search Strategy

A majority of the information referenced for this study consists of peer-reviewed journal articles relevant to cyberterrorism with an emphasis on research from 2016 to 2020. I primarily conducted research through online databases consisting of Academic

Search Complete, Political Science Complete, Google Scholar, SAGE Premier, and ProQuest Central. I used Ulrich Periodicals to ensure that journals referenced in this study were peer-reviewed. The database search terms included *cyberattack*, *cybercrime*, *cyberterrorism*, *cyberwar*, *hacking*, *information warfare*, *international*, *laws, NATO*, *national security*, *punctuated equilibrium theory*, *responses*, *state-sponsored*, *terrorism*, *United Nations*, and *United States*. One hundred and twelve peer-reviewed studies from 2016 to 2020 supported the findings of the literature review and this study.

Theoretical Foundation

Overview and Key Framework Proposition

Democratic political processes are outwardly associated with long periods of relative stability. These governments follow rules and regulations for electing officials, formulating laws, and governing citizens. Yet, government operations during disasters, such as 9/11, shift to crisis management which often becomes the catalyst for rapid political change. Punctuated equilibrium theory shows that stability and change are important aspects of the political process and includes both into its framework (Baumgartner et al., 2018; Kuhlmann & Van der Heijden, 2018).

In this study, I used punctuated equilibrium theory to review the validity of improving U.S. cyberterrorism deterrence and response options. Cyberterrorism guidance is created by policymakers in either relative stability before a cyberterrorism attack or within an excited environment following a successful cyberterrorism attack. Terrorism and cybersecurity experts cannot make changes to U.S. policy without policymaker concurrence. These experts, therefore, must observe and navigate U.S. government institutional friction described by punctuated equilibrium theory in order to offer improvements for cyberterrorism deterrence and response guidelines. They must additionally work with policymakers for any cyberterrorism response plan drafted in the chaotic environment following a large-scale cyberterrorism attack. I used punctuated equilibrium theory to conceptualize expert cyberterrorism deterrence and response plan improvements in these two very different environments.

Punctuated equilibrium theory draws from political science approaches acknowledging that political processes mostly operate in stable environments defined by measured progress (Baumgartner et al., 2018; Koski & Workman, 2018; Noone, 2019). Yet, these same enviroments can also experience decisive change to resolve large political problems (Baumgartner et al., 2018; Noone, 2019). Punctuated equilibrium theory states that decisions are made through *bounded rationality* or within the cognative abilities and timeframes of policymakers and organizations (Kuhlmann & Van der Heijden, 2018). The theory emphasizes *issue definition* and *agenda setting* with respect to the policy process to help quantify the variation in change (Baumgartner et al., 2018; Koski & Workman, 2018).

Issues are addressed by priority in public agendas to either reinforce or question standing polices (Baumgartner et al., 2018; Koski & Workman, 2018). Reinforced policies can only be margionaly reformed, yet questioned policies can create an atmosphere for large change (Baumgartner et al., 2018). However, even when change is evident, institutional friction can present a barrier by making the policy change process difficult (Flink, 2017; Koski & Workman, 2018). This friction causes pressure to build which leads to a *punctuation* overtime (Flink, 2017; Koski & Workman, 2018). Punctuated equilibrium theory thus also offers reasoning for the sudden shifts in policy change.

Punctuated equilibrium theory was created to be widely applied to many policy venues and is recognized in the United States and throughout the world (Koski & Workman, 2018). Since 1993 the theory has appeared in 90 mostly U.S.-based journals covering public administration, public policy, U.S. politics, and comparative politics (Baumgartner et al., 2018; Kuhlmann & Van der Heijden, 2018). Kuhlmann and Van der Heijden (2018) identified 86 high quality articles not written by the punctuated equilibrium theory's creators covering topics ranging from budget change, health, environmental and energy policy, tobacco policy, and education policy (Flink, 2017; Kuhlmann & Van der Heijden, 2018).

Literature Review Related to Key Concepts

Communication and the flow of information play important roles in virtually all aspects of life and are integral for collective security and stability (Osawa, 2017). Nearly half of the world's population is connected to the internet with access to information available through infrastructure consisting of networks, software, and facilities (Nye, 2017; Shad, 2018). However, increasing worldwide dependence on cyberspace has exposed mounting malicious cyber activities which has raised security concerns (Nye, 2017; Osawa, 2017).

Cyberattacks can be classified as either exploitation attacks on computer systems or destructive physical attacks using computer systems (Shad, 2018). The main culprits of cyberattacks are states, terrorist groups, terrorist sympathizers, anti-government hackers, and thrill-seekers (White, 2016). Taken wholly, the internet provides a massive target for criminals operating in relative safety to cause damage and disruption far exceeding any conventional attack (Albahar, 2019). In fact, a successful large-scale cyberattack could cost the United States upwards of $50 billion USD which is comparable to a severe natural disaster (Osawa, 2017). Cyberspace is still a largely unregulated domain and cybercriminals and cyberterrorists will continue to conduct increasingly brazen attacks and exploit cyberspace to their advantages until comprehensive policies are drafted to address these threats.

Rationale and Relevance of Framework

Punctuated equilibrium theory is relevant for justifying cyberterrorism deterrence and response plans during periods of relative stability before a successful large-scale cyberterrorism attack as well as in an environment primed for rapid political change following an attack. This theory is also relevant when comparing its concepts of constrained agendas and the cognitive ability limits of policymakers to the long attribution process and technical nature of cyberattacks. Data extracted through expert interviews clarified any past cyberterrorism policy attempts. Punctuated equilibrium theory also highlights the many barriers for successful political change as well as the reasoning for the rapid implementation of the Patriot Act following 9/11, which significantly altered U.S. counterterrorism guidelines. Finally, punctuated equilibrium theory was used as a lens to understand the relationship between policy information flow and political change to guide this study.

Punctuated equilibrium theory has been the chosen methodology for 59 peer-reviewed journal articles with 66% of these articles published from 2010 to mid-2020. Yet, punctuated equilibrium theory related to terrorism, cyber, and security all yielded zero search returns in multiple academic peer-reviewed databases. However, punctuated equilibrium theory was the chosen methodology for eight publicly available terrorism dissertations, 84 policy dissertations, and eight security dissertations with 69% published from 2010 to mid-2020. Therefore, punctuated equilibrium theory is predominately coupled with policy focused peer-reviewed journal articles and dissertations, as was this study, and has been growing in popularity since its 1993 advent.

Cyberwarfare

There is currently no consensus on what defines a cyberwar or when a cyberattack could be considered an armed attack. Further debate arises on if a cyberattack constitutes a *casus belli* or if just war theory would apply to cyberconflict (Sleat, 2017). States must currently defer to domestic and international guidelines relating to cybercrime and armed conflict for guidance since no binding international frameworks exist to address cyberwarfare. The difficulty to apply laws that were created before the invention of computers while considering the complex nature of cyberspace will limit the abilities of some states to act while others will use the inevitable ambiguities for their own advantages (Fenton, 2019).

International Reception

Multilateral institutions are largely incapable of addressing the evolving issues of cyberspace related crime and conflict. The Council of Europe's Convention on

Cybercrime, also known as the Budapest Convention, is currently the only binding international treaty dedicated to cybercrimes (Van Dine, 2020). The intent of the Budapest Convention is to provide a common legal basis to minimize barriers for international prosecution (Van Dine, 2020). Since 2004 64 states including the United States have ratified the Budapest Convention. Signature parties have integrated aspects of this Convention into their own domestic laws, yet the Convention's main purpose is to offer frameworks for states to use as guidelines to construct their own cyber related criminal legislation (Van Dine, 2020). The two international groups most active in defining cyberwarfare standards are the United Nations (UN) and the North Atlantic Treaty Organization (NATO; Mazanec, 2016).

UN

Article 2(4) of the UN Charter prohibits the use of force or the threat of force against another state (UN, 1945). This Article essentially bans UN members from using force on all but the two following conditions articulated by the Charter. Article 42 states that force can be used when the Security Council authorizes it in order to restore peace (UN, 1945). Additionally, Article 51 permits using force for the purposes of individual or collective self-defense following an armed attack (UN, 1945). An *armed attack* is viewed as a higher level of transgression than *use of force* highlighted in Article 2(4) (Dev, 2015). It is generally accepted that a state can exercise its right to self-defense in Article 51 following a cyberattack if that attack meets *armed attack* thresholds (Dev, 2015). Yet, legal ambiguities exist on whether Article 2(4) and Article 51 apply to non-state actors conducting cyberterrorism attacks (Efrony & Shany, 2018). There is also uncertainty on when a cyberattack would be considered *use of force* prohibited by Article 2(4) (Efrony & Shany, 2018). However, the UN occasionally clarifies cyber related Charter ambiguities with policy releases.

In 2013 the UN adopted cybercrime and cybersecurity principles to standardize policy and facilitate UN assistance for cyberspace related issues (Dorn, 2018). In 2014 the UN declared that self-defense could be used in response to a cyberattack under Article 51 of the UN Charter (Hodgkinson, 2018). Yet, discussions in 2017 concerning responsible state behavior in cyberspace failed to produce a report or even reach an agreement (Boeke & Broeders, 2018).

The UN is currently composed of 193 Member States, omitting only the Holy See (metonymically known as Vatican City) and Palestine. Not surprisingly then, worldwide consensus on vague or controversial topics can be difficult. Additionally, the 15 member UN Security Council must unanimously agree to adopt resolutions. The five permanent members of the Security Council are China, France, Russia, the United Kingdom, and the United States. The varying ideologies of these governments make unanimous agreements on cyberspace measures problematic. However, NATO is an international organization better suited to respond to cyberspace related issues given its collective defense conception.

NATO

NATO is a military alliance consisting of 30 North American and European states. The Alliance opened the Cyber Defence Center of Excellence in Tallinn, Estonia in 2008 one year after a 3-week long suspected Russian cyberattack against the country

(László, 2018; Marsili, 2019). NATO subsequently made cyber defense and preparing for cyberspace conflict a priority at the Alliance's 2010 Lisbon Summit (László, 2018). NATO implemented additional cyber related policies, plans, and response cells at the 2012 Chicago Summit (László, 2018). Following this Summit, NATO's Cyber Defence Center of Excellence released the *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013 which is now used as a basis for all cyber actions (László, 2018).

The Tallinn Manual contains cyber conflict and security topics including sovereignty, *jus ad bellum*, and international humanitarian law as interpreted by international experts (Barrett, 2017; László, 2018; Marsili, 2019). The manual addresses the difficulties of legally framing cyberattacks as well as defining attacks as criminal or political and attributing them to state or non-state actors (Marsili, 2019). An updated and significantly expanded "Tallinn Manual 2.0" was released in 2017 which also explores how international law relates to peacetime cyber operations and to cyberattacks that would not be considered armed attacks (Efrony & Shany, 2018; Hodgkinson, 2018; Marsili, 2019).

At the 2014 NATO Summit in Wales, the Alliance agreed that international law extended to cyberspace and acknowledged that cyberattacks could be as dangerous as conventional attacks thereby making cyber defense an integral part of NATO's collective security (Hodgkinson, 2018; Marsili, 2019; Osawa, 2017). As a result, cyberattacks against a member state meeting armed attack criteria would invoke Article 5 which requires NATO to collectively aid any attacked member (Hodgkinson, 2018; Marsili, 2019). Finally, NATO elevated cyberspace to a fourth operational dimension of warfare along with air, sea, and land at the Alliance's 2016 Warsaw Summit (László, 2018; Marsili, 2019). The United States, NATO's primary partner, has created cyber policy largely in parallel with NATO to both enhance international cooperation and to unilaterally address cyberthreats.

United States' Reception

U.S. technological innovation was accelerated by the rapid electronic developments following World War II (Bracken, 2017). New inventions improved many individual and collective aspects of the country. Yet, the proliferation of technical knowledge was also inevitably used for nefarious purposes.

The United States first addressed concerns regarding U.S. networked computer systems in President Ronald Regan's 1984 National Security Decision Directive 145 which acknowledged that networked systems were vulnerable to exploitation and called for a plan to secure them (Boys, 2018). By the mid-1980s it became clear that foreign governments and terrorist organizations were in fact infiltrating networked computer systems throughout the United States (Boys, 2018). In the early-1990s the U.S. National Research Council and the National Academy of Sciences reiterated U.S. computer vulnerabilities and identified the possibility of a deliberate cyberattack against the country (Boys, 2018). President George H.W. Bush addressed these concerns in National Security Directive 42 which outlined a coordinated national security defense structure to guard against foreign threats (Boys, 2018; Tabansky, 2018).

By the mid-1990s government officials began to recognize the significant cyberspace risks to U.S. national security and President Bill Clinton signed six cybersecurity related executive orders from 1993 to 1999 (Boys, 2018). These executive orders created various organizations to address a range of developing issues including information networks, foreign access to U.S. technology, critical infrastructure protection, encryption export controls, and internet regulation (Boys, 2018). Yet, President Clinton's most comprehensive cybersecurity document was Presidential Decision Directive 63, released in 1998, that created directorates, offices, and groups to ensure economic and critical infrastructure cyberspace protection (Boys, 2018). This Directive also highlighted cyberwarfare as a threat to U.S. military superiority (Boys, 2018; Tabansky, 2018).

Cyberspace rapidly expanded throughout the 1990s as the popularity of personal computers and the internet increased worldwide. President George W. Bush released the *National Strategy to Secure Cyberspace* in 2003 which called for private and public cooperation to create an emergency response system for cyberattacks (Wilner, 2020). He also released the still classified National Security Presidential Directive 38 relating to cyberspace security that same year (Wilner, 2020). President Bush expanded his 2003 Cyberspace Strategy in the 2008 Comprehensive National Cybersecurity Initiative established by National Security Presidential Directive 54 (Wilner, 2020). This Initiative provisioned cybersecurity roles to government agencies such as U.S. government network protection to the Department of Homeland Security, attack deterrence to the Department of Defense, information coordination to the Federal Bureau of Investigation, and counterintelligence development to the Director of National Intelligence (Wilner, 2020). Present Barack Obama made cybersecurity a priority and expanded and completed

President Bush's Comprehensive National Cybersecurity Initiative in 2009 with the creation of the U.S. Cyber Command under the Department of Defense to unify and strengthen cyberspace operations (Wilner, 2020).

President Obama's 2011 *International Strategy for Cyberspace* stated that the United States will use all necessary means for cyberattack defense but will limit military force as a last resort (Mazanec, 2016; Wilner, 2020). President Obama combined this Strategy with his 2012 top-secret Presidential Policy Directive 20 (made public by Edward Snowden in 2013) outlining a cybersecurity framework to establish principles and processes for offensive U.S. cyber capabilities (Hodgkinson, 2018; Marsili, 2019). Finally, President Obama reiterated strengthening critical infrastructure cybersecurity frameworks with Presidential Policy Directive 21 in 2013 as well as in his 2015 National Security Strategy (Kosseff, 2018; Tabansky, 2018). Cyberspace security was perceived to be a very real threat in the United States following Russian interference in the 2016 U.S. presidential election, and President Donald Trump continued to strengthen U.S. cybersecurity frameworks created by his predecessors after taking office.

President Trump issued Executive Order 13800 on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* four months after his 2017 inauguration to grow and sustain a cybersecurity workforce to achieve cyberspace objectives (Marsili, 2019; Osawa, 2017). President Trump then released the *National Cyber Strategy of the United States of America* a year later in 2018 which updated President Bush's 2003 *National Strategy to Secure Cyberspace* (Wilner, 2020). Following Executive Order 13800 and the 2018 Cyber Strategy, the Department of State released presidential guidance for prioritizing cyberthreats in domestic and foreign policy and strengthening international cyberspace cooperation (Marsili, 2019; Wilner, 2020). Finally, in 2018 President Trump rescinded Presidential Policy Directive 20 to loosen restrictions that President Obama had placed on cyber operations while also elevating Cyber Command to one of the Department of Defense's eleven Unified Combatant Commands (Marsili, 2019; Wilner, 2020). Presidential directives, executive orders, and strategies assign cyberspace related tasks to many U.S. government departments. Yet, the three departments leading U.S. cyberspace policy and execution are the Department of Defense, the Department of State, and the Department of Homeland Security.

The Department of Defense is predictably responsible for the defense of cyberspace and the deterrence of cyberattacks. Like NATO, the Department of Defense views cyberspace a separate operational domain (Marsili, 2019; Tabansky, 2018). However, the Department of Defense is subservient to the Department of Homeland Security concerning domestic cyber operations and can only act after the Department of Homeland Security requests assistance following an emergency in accordance with the U.S. Defense Support of Civil Authorities (Tabansky, 2018).

The Department of Homeland Security is therefore responsible for guarding domestic U.S. computer networks from threats. Specifically, the Department of Homeland Security protects civilian government information systems with assistance from agencies such as the Federal Bureau of Investigation under the U.S. Department of Justice and through the Central Intelligence Agency as part of the greater 16 agency U.S. Intelligence Community (Marsili, 2019; White, 2016). The Department of Homeland

Security does share cyber related information with the private sector, yet the Department cannot regulate private cyber processes (Kosseff, 2018).

While the Department of Homeland Security is concerned exclusively with domestic cyber matters, the Department of State concentrates on international engagement. In line with its diplomatic purpose, the Department of State promotes an open and secure cyberspace to support cyberspace goals and shape cyber norms worldwide. The Department of State did create the Office of the Coordinator for Cyber Issues to address international cyberspace related issues and acceptable behaviors, yet that office was disbanded in February 2018 by then Secretary of State Rex Tillerson and has not yet been replaced as of 2020 (Marsili, 2019).

United States' Cyber Evolution

The National Security Agency began exploiting computers and networks as early as 1985, realizing that they must keep pace with dynamic computer and information technological advances (Loleski, 2019). In 1994 the Agency began to define *information intelligence* and *computer intelligence* as an offshoot to the already established *signals intelligence* on which the Agency was founded (Loleski, 2019). Still, in 1997 the Senate Intelligence Committee questioned the National Security Agency's ability to adapt to technological advancements in a punitive report (Loleski, 2019). As a result, in 1999 the National Security Agency began agency wide reorganization and replaced their passive signals intelligence collection concept with a new active digital hacking network intelligence concept (Loleski, 2019).

United States cyber espionage operations were largely made public through Julian Assange's WikiLeaks and through former National Security Agency contractor Edward Snowden (Shad, 2018; Hellmuth, 2018a). Information amongst the hundreds of thousands of classified documents that WikiLeaks released in 2010 suggested that the United States was spying on foreign government officials (Shad, 2018). Further, Snowden's 2013 leaks revealed that the United States conducted thousands of cyber operations against both hostile and friendly states (Hellmuth, 2018b; Shad, 2018). Finally, it is assumed that the United States and Israel were responsible for the Stuxnet computer virus in 2010 that damaged centrifuges at Iran's Natanz nuclear facility which likely caused significant damage to Iran's nuclear program (Nye, 2017; Shad, 2018). The Stuxnet attack is notable because it was the first cyberattack to cause physical damage to a government operated critical infrastructure facility (Dinniss, 2018; Osawa, 2017).

Notable States' Cyber Praxes

States are increasingly exploiting cyberspace to achieve political and military objectives including information operations, espionage, propaganda, and attacks against critical infrastructure (Shad, 2018). A wide range of cyberattacks occur against an even wider range of targets throughout the world. More than 10 million daily attacks are attempted against the Pentagon alone (Nye, 2017). A vast majority of these cyberattacks are inconsequential, yet some are destructive and demand the attention of governments to formulate potential responses (Nye, 2017). Security experts believe that the United States, the United Kingdom, Israel, Russia, and China have the ability to conduct offensive cyber operations and are thus known as *cyber superpowers* while North Korea and Iran are also aggressively pursuing offensive cyber capabilities (Shad, 2018).

Russia

Russia has demonstrated on multiple occasions that it will continue to conduct cyber operations against a range of targets in many different countries (Mazanec, 2016). Cyberwarfare is an important aspect of Russian military operations and the country invests immense amounts of resources to increase cyberattack capabilities (Baram & Menashri, 2019). Russia initially limited its cyberattacks to post-Soviet states but has also begun to engage the West following President Vladimir Putin's rise to power in 2012 (Shad, 2018).

In fact, the first instance of a state-sponsored cyberattack was conducted by Russia against Estonia in 2007 which stemmed from Estonia's removal of a Red Army statue (Hodgkinson, 2018; Osawa, 2017). Russia responded with a series of cyberattacks by successfully shutting down many of Estonia's important government and institutional websites as well as all banking services for two of Estonia's largest banks (Osawa, 2017). A year later, in 2008 Russia was accused of a more complex cyberattack that compromised over 300 Lithuanian websites with pro-Russian messages and symbols (Osawa, 2017). Also, in 2008 vast denial-of-service attacks, or information flooding, were seen in Georgia to coincide with the invasion of Russian troops which shut down many important websites (Nye, 2017; Osawa, 2017). Lastly, in 2009 Kyrgyzstan's two largest internet companies providing over 80% of the country's internet received sustained Russian denial-of-service attacks and were forced to temporarily cut service (Osawa, 2017).

Russia was again accused of a series cyberattacks, this time against Ukraine, in 2015 following the annexation of Crimea (Kosseff, 2018; Osawa, 2017). Russia initially targeted a power grid company which caused 225,000 Ukrainian citizens to temporarily lose power on Christmas Day (Nye, 2017; Osawa, 2017). This attack was notable because it was the first proven cyberattack by one country against the critical infrastructure of another (Osawa, 2017). A similar cyberattack occurred a year later in 2016 in the Ukrainian capital of Kiev after which Ukraine declared that Russia was conducting a cyberwar against them (Osawa, 2017). Still, Ukraine was again attacked six months later in 2017 (Efrony & Shany, 2018; Osawa, 2017). This cyberattack was known as the Petya/NotPetya attack and targeted Ukrainian government agencies, banks, power grids, and railway and subway systems (Efrony & Shany, 2018; Osawa, 2017). Petya/NotPetya spread globally and affected more than 60 countries, including the United States, and companies reported losses in the hundreds of millions of dollars (Efrony & Shany, 2018). The United States called this cyberattack the most costly and destructive in history up to that point (Efrony & Shany, 2018). At the same time Russia was interfering with Ukrainian computer networks, they were also directly targeting United States' systems.

Russia was accused of manipulating public opinion to sway the 2016 U.S. presidential election by using social networking services to display fake media and by leaking inside information against the Democratic National Committee (Osawa, 2017). Russia also hacked into voting related databases and systems in 39 U.S. states (Kosseff, 2018). The United States accused Russia of state involvement in these cyberattacks and released a report directly identifying President Putin as the approver (Shad, 2018). As a result, President Obama expelled 35 Russian diplomats from the United States, closed two Russian backed facilities, and levied targeted economic sanctions against Russia itself (Efrony & Shany, 2018; Shad, 2018; Wilner, 2020). In fact, from 2007 to 2017 there were 34 known state-sponsored cyberattacks including eight against the United States (Osawa, 2017).

In 2018 the Department of Homeland Security and the Federal Bureau of Investigation warned that, beginning in 2014, Russian government cyber actors had targeted many aspects of U.S. critical infrastructure such as water supply, aviation, and nuclear power plant systems of which 90% are privately owned (Weiss & Jankauskas, 2018). Following this revelation, the United States imposed sanctions and indictments against 12 Russian Main Intelligence Directorate (GRU) operatives, Russian government hackers, and 17 government officials with close ties to President Putin (Efrony & Shany, 2018).

China

China initially developed and expanded its military cyber capabilities to use for asymmetrical advantages (Baram & Menashri, 2019). Yet, the country now incorporates cyber technologies in all national security initiatives in the economic, diplomatic, and military realms (Mazanec, 2016). China’s cyber capabilities are thus postured for economic damage, critical infrastructure attacks, and kinetic conflict (Mazanec, 2016).

However, China only regularly conducts cyber espionage and, unlike Russia, has shown restraint in damaging cyberattacks (Mazanec, 2016).

The U.S. government believes China began conducting U.S. intellectual property theft through cyberspace as early as 2002 including intrusions in the Department of Defense network (Mori, 2019). In fact, a 2013 investigation uncovered at least 141 Chinese military cyberattacks against U.S. government and civilian agencies (Mazanec, 2016). Many other countries also accuse China of cyber espionage including Australia, Canada, and India. The United States classified China as the most active international perpetrator of espionage in 2014 after five Chinese military hackers were indicted by the Department of Justice for cyber exploitation within the United States (Mazanec, 2016).

In 2015 the United States and China appeared to come to agreement on certain aspects of cybercrime by mutually banning intellectual property theft, yet there was no mention of cyber espionage which both countries generally recognize as fair game (Mazanec, 2016). However, there is evidence that China's exploitation cyberattacks against the United States continue and China is thus still considered the main cyber threat to the United States (Mazanec, 2016; Tabansky, 2018). Because of this, since 2018 the United States has shifted away from engagement and even imposed a series of tariffs on China that affected 67% of Chinese imports while China reciprocated by levying tariffs on 60% of U.S. imports (Congressional Research Service, 2019; Mori, 2019).

North Korea

North Korea has been developing offensive cyber weapons mainly to augment its outdated conventional military force (Boo, 2017). North Korea is one of the poorest countries in the world with only a few thousand computers connected to its rudimentary internet (Boo, 2017). Yet, the country has still been able to launch complex cyberattacks against the United States and South Korea (Boo, 2017).

In 2013 South Korea faced a sophisticated cyberattack against its television stations and three major banks which were taken offline for several hours (Osawa, 2017). South Korea blamed North Korea for the attack which occurred during increased tensions on the Korean Peninsula (Osawa, 2017). A year later, in 2014 North Korea infiltrated nearly half of Sony Pictures Entertainment's computers and servers located in the United States and publicly released scores of confidential information which resulted in the United States levying additional sanctions against the country (Kosseff, 2018; Osawa, 2017; White, 2016). These North Korean hackers, known as Guardians of Peace, were also accused of cyberattacks against South Korean targets, including a nuclear power plant, in 2015 and 2016 (Efrony & Shany, 2018). Lastly, North Korea was blamed for the 2017 WannaCry cyberattack which affected hundreds of thousands of computers in over 150 countries including Russia, China, the United States, and the United Kingdom (Efrony & Shany, 2018). This ransomware attack encrypted data on affected systems which could only be unlocked with a Bitcoin ransom payment (Efrony & Shany, 2018).

Iran

From 2011 to 2013 the United States witnessed a total of 176 days of Iranian cyberattacks against 46 U.S. financial institutions including the New York Stock Exchange, the Bank of America, Wells Fargo, and AT&T (Efrony & Shany, 2018). The cyberattacks, known as Operation Ababil, were conducted by a self-proclaimed Arab

Muslim group named Izz ad-Din al-Qassam Fighters (Efrony & Shany, 2018). In 2016 the United States accused Iran’s Islamic Revolutionary Guards Corps of these attacks in addition to infiltrating the command and control systems of the Bowman Dam in New York three years earlier (Hodgkinson, 2018). However, the head of Iran’s cyber police denied responsibility for these attacks (Efrony & Shany, 2018).

Iran was also suspected of accessing Sands Casino computer systems in 2014 which significantly affected the casino’s operations (Efrony & Shany, 2018). The casino’s owner, Sheldon Adelson, stated a year earlier that he wanted to detonate a nuclear bomb in the Iranian desert to demonstrate U.S. strength which was likely the catalyst for the cyberattack (Efrony & Shany, 2018). The Sands Casino cyberattack occurred nine months before North Korea’s Sony Entertainment cyberattack making the Ababil operation the first destructive cyberattack by a state against a private U.S. company (Efrony & Shany, 2018).

Terrorism

By the late 19th century, advances in technology and communication offered inexpensive travel and near instantaneous information flow (Rapoport, 2016). These advances, in part, allowed the rise of global terrorism which began in the 1880s with the spread of the Russian anarchist movement to other countries (Rapoport, 2013). The end of the 19th century witnessed many anarchist motivated shootings and bombings which included the assassinations of a French president and an Italian king (Hughes, 2011). Yet, Russian Tsar Alexander II’s assassination in 1881 was the most famous and inspired revolutionary violence throughout the country and subsequently the world (Hughes, 2011). However, the anarchist movement was only the beginning element of modern terrorism.

David Rapoport (2013) argued that the world has subsequently witnessed three new characterizations of terrorism that developed throughout the 21st century with the emergence of ani-colonialism terrorism, revolutionary terrorism, and the current religious terrorism. He explained that each of these *waves* last approximately a generation and appear in expansion and contraction cycles, including the current religious wave (Rapoport, 2013). A wave contracts when organizations can no longer inspire successor groups, or groups change tactics to become relevant in another wave (Rapoport, 2013). However, organizations can also transcend multiple waves such as the still active Irish Republican Army which emerged in 1916 (Rapoport, 2013).

The main goal of every terrorist organization in every wave is revolution to either encourage national self-determination, construct a new form of authority, or inspire a new source of legitimacy (Rapoport, 2013). Religion has always played an important role in modern terrorism since ethnic and religious identities often overlap (Rapoport, 2013). However, the current wave of religious terrorism is centered around Islam and aims for a religious state as opposed to a secular one (Rapoport, 2013). Yet, there are still many active and dangerous nonreligious terrorist groups including state-sponsored terrorist organizations. For example, nonreligious terrorist groups make up approximately 20% of the U.S. Department of State's Foreign Terrorist Organizations list containing over 80 different groups as of 2020 and should thus also be considered in U.S. counterterrorism guidelines (Bureau of Counterterrorism, n.d.).

States began drafting legislation against terrorism related acts in the 18th century stemming from the French Revolution of 1789 to 1799 (Rich, 2013; Shor, 2016). Laws largely included the term *terrorism* by the 20th century, and a new wave of counterterrorism legislation appeared in the 21st century following the attacks of 9/11 (Shor, 2016). Seventeen international conventions have convened since 1920 to discuss terrorism, yet none developed an agreed definition of the term reflecting states' desires to retain domestic control of the meaning to preserve unilateral response options (Fidler, 2016; Marsili, 2019). Terrorism then is a subjective term that has evolved over time and varies in meaning depending on the endorsing party (Hellmuth, 2018b). Yet, terrorism is generally defined as violence against civilians by non-state actors to obtain a political objective (Gaibulloev & Sandler, 2019; Hoffman, 2017). Examples of terrorism include politically motivated bombings, kidnappings, armed attacks, and assassinations (Gaibulloev & Sandler, 2019).

Modern terrorism research began in the 1960s and 1970s focusing on Algeria and Indochina (Rich, 2013; Roberts, 2015). Terrorism and counterterrorism literature have continued to grow and are now included in the studies of international relations, politics, history, and sociology (Roberts, 2015). However, terrorism study is still controversial which is highlighted by the fact that no absolute terrorism definition exists (Hoffman, 2017; Roberts, 2015). Additionally, terrorism methodologies are also questioned since researchers are unable to produce significant datasets on individual terrorists which leaves the data open to criticism (Roberts, 2015).

There are also conflicting opinions on the effectiveness of counterterrorism legislation (Shor, 2016). Some believe this legislation allows states to protect themselves by drafting response plans for both preemptive deterrence and to rapidly execute following an attack (Shor, 2016). Others feel that counterterrorism legislation has no effect on terrorist actions and that countries mainly adopt these policies for a variety of political reasons other than fighting terrorism (Shor, 2016). A final group believes that counterterrorist legislation makes terrorism worse since the legislation violates human rights, creates criticisms, and advertises post-attack responses to potential adversaries (Shor, 2016).

International Response

Direct conflict amongst states has largely given way to proxy wars and state-sponsored terrorism since the mid-20th century. The United States has been in scores of conflicts since World War II but most recently issued a war declaration in 1942 against Bulgaria, Hungry, and Romania. Additionally, terrorist organizations have risen from within states to counter what they view as outside threats or internal suppression. The UN Charter's first purpose is to maintain peace and security worldwide, and the Organization has realized the need to adapt to evolving international conflicts (UN, 1945). The UN has therefore updated their doctrine to counter terrorist organizations in order to fulfil their Charter obligations (Hansen et al., 2020).

The UN first discussed terrorism in September 2001 with Security Council Resolution 1373 that established a mandate for all member-states to address terrorism (Karlsrud, 2017). Further, the Responsibility to Protect Doctrine drafted in 2005 and the

Global Counter-Terrorism Strategy created in 2006 improved civilian protection and peacekeeper integration for UN counterterrorism efforts (Hansen et al., 2020; Karlsrud, 2017). The UN's definition of terrorism also changed to *violent extremism* and, in 2015, then UN Secretary-General Ban Ki-moon issued his *Plan of Action to Prevent Violent Extremism* (Karlsrud, 2017). UN peacekeeping missions have likewise evolved to aid counterterrorism efforts (Karlsrud, 2017).

The UN Multidimensional Integrated Stabilization Mission in Mali, deployed in 2013, was the first insertion of a UN peacekeeping force during an already ongoing counterterrorism operation (Karlsrud, 2017). UN forces, working closely with the French operation, were tasked with regaining control of terrorist held areas in Mali (Hansen et al., 2020; Karlsrud, 2017). The UN has therefore been in ongoing and open conflict with various terrorist groups and has suffered 227 fatalities as of October 2020 making the Mali mission the deadliest in UN history (*Fatalities*, n.d.; Hansen et al., 2020).

NATO has also played a role in expanding global counterterrorism frameworks in line with UN policies (Federica, 2018). The Alliance accepted its first Military Concept for Defence against Terrorism in 2002 in reaction to Article 5's invocation (Federica, 2018). NATO further released its Counter Terrorism Policy Guidelines in 2012 focusing on building capabilities and strengthening partner engagement and created a robust Action Plan in 2017 to review NATO's current counterterrorism strategy and recommendations for future actions (Federica, 2018). The Military Concept for Defence against Terrorism was updated in 2015 to include the 2006 UN Global Counter Terrorism

Strategy and the 2012 Policy Guidelines which allows NATO to contribute more efficiently to counterterrorism operations (Federica, 2018).

In 2016 NATO acknowledged that terrorism represented a direct threat to all member states which led to the 2017 Action Plan (Federica, 2018). This plan recognizes that every state has different approaches to terrorism and thus allows states to retain authority for their own domestic security while offering ways that the Alliance can still provide value (Federica, 2018). Since 2017 NATO has taken many steps to counter terrorism threats including establishing a Terrorism Intelligence Cell, creating a common biometric data policy, and generally working with regional and international organizations such as the UN, the European Union, and the African Union to improve cooperation efforts (Federica, 2018). The Action Plan, updated in 2018, also continues to support military operations in Afghanistan that began with the International Security Assistance Force in 2001 (Federica, 2018).

The UN Security Council established the NATO led International Security Assistance Force in December 2001 with Resolution 1386 which was initially focused on Kabul, Afghanistan but spread throughout the country by 2006 (Hellmuth, 2018a). This mission concluded in 2015 and was replaced with the Resolute Support Mission which is considered a non-combat training operation for Afghanistan’s security forces and institutions (Federica, 2018). NATO has also been training and advising members of Iraq’s government and military since 2018 at the request of the country’s prime minister (Federica, 2018). In fact, NATO forces have been conducting counter-ISIS operations in

Iraq since 2015 which was officially sanctioned by the Alliance's 2017 Action Plan (Federica, 2018).

United States' Response

Terrorism has become a household name in the United States as a result of 9/11. The word *terrorism* itself invokes strong feelings for many U.S. citizens shaped by personal experiences and patriotism. Whether through ignorance or apathy, the U.S. government has not accurately defined or categorized terrorism amongst its many laws and guidelines despite the term persisting for as long as the United States itself.

The United States reduced terrorism research funding following the collapse of Soviet Union affiliated terrorist organizations in the 1990s despite the proliferation of religious terrorist groups beginning in the 1980s (Hellmuth, 2018a; Rapoport, 2016). Consequently, U.S. government reports attributed the 1998 U.S. embassy bombings in Tanzania and Kenya and the 9/11 attacks partially on government indifference toward terrorist organizations (Rapoport, 2016).

In retaliation for the embassy attacks, the United States bombed a training camp in Afghanistan and a pharmaceutical plant in Sudan (Hellmuth, 2018a). However, this was an exception to U.S. counterterrorism policy at the time since the 1996 Khobar Towers bombing in Saudi Arabia by Hezbollah and the al Qaeda led suicide attack against the USS Cole in 2000 only generated criminal investigations and indictments (Hellmuth, 2018a). However, the United States response to the 9/11 attacks was swift and aggressive and would have lasting consequences for years to come when combined with the political fallout and subsequent military interventions that followed.

The United States has concentrated on preventing terrorism from reaching its borders since 2001 through multiple invasions, housing detainees offshore, and creating sweeping legislative reform (Hellmuth, 2018a; Roberts, 2015). The Patriot Act was passed six weeks after 9/11 making terrorism data collection and cross-agency information sharing improvements as well as expanding investigative authority for government agencies (Hellmuth, 2018a). In November 2001 President Bush signed a Military Order authorizing convictions through military commissions and indefinite detention of al Qaeda detainees at Guantanamo Bay, Cuba (Hellmuth, 2018a). Further, the Department of Homeland security was created in November 2002 which consolidated 22 domestic protection agencies such as the U.S. Coast Guard, the Secret Service, and the Transportation Security Administration (Hellmuth, 2018a). The last initial reform was the 2004 Intelligence Reform Act that broadly affected U.S. federal terrorism laws and established the cabinet-level position of the Director of National Intelligence to coordinate U.S. intelligence efforts (Hellmuth, 2018a). Yet, the country did meet internal resistance to some counterterrorism measures.

The executive branch’s 2002 Homeland Security Act, 2005 Patriot Reauthorization Acts, and 2008 Foreign Intelligence Surveillance Amendment Act all met some form of congressional resistance (Hellmuth, 2018a). Additionally, in 2004 the U.S. Supreme Court established jurisdiction in Guantanamo Bay by agreeing that detainees had *writ of habeas corpus* rights, or determining the validity of detention, and also required a mandate for the military commissions prosecuting detainees (Hellmuth, 2018a). Congress subsequently passed the 2006 Military Commissions Act in an attempt to counter these Supreme Court measures (Hellmuth, 2018a).

The United States also began more closely monitoring border security and tightening visa programs as measures to keep potential terrorists out of the country (Hellmuth, 2018a). Additional programs were created or improved to monitor the status of foreigners once in the country such as the 2003 Student and Exchange Visitor Information system to track foreigners, the 2004 Visitor and Immigrant Status Indicator Technology program to store biometric data, and the 2009 Electronic System for Travel Authorization approval program (Hellmuth, 2018a). Other measures included no-fly lists and physical border fences (Hellmuth, 2018a). All initial government effort was focused on keeping foreign terrorists out of the United States and closely monitoring foreigners suspected of being terrorists.

The United States did not begin focusing on domestic religious terrorism until 2009 (Hellmuth, 2018a). However, 16 Islamic lone-wolf terrorism attacks have been attempted in the United States since 2009 including the 2013 Boston Marathon bombings and the 2015 and 2016 mass shootings in San Bernardino and Orlando, respectively (Hellmuth, 2018a; Jasko et al., 2017; Rapoport, 2016). The only surviving perpetrator of these attacks was Dzhokhar Tsarnaev who was found guilty of using a weapon of mass destruction and causing damage to property resulting in death.

Other notable domestic but non-religious terrorism shootings included the 2015 Charleston church shooting by a white supremist and the 2017 congressional baseball shooting by a political opponent. U.S. domestic terrorist attacks in the first two decades of the 21st century were either lone-wolf attacks or conducted by a few individuals. Because of this, reactions focused mainly on gun control measures as opposed to increased counterterrorism actions. This observation is relevant since a destructive U.S. cyberterrorism attack could also be conducted by a lone-wolf domestic terrorist, and the internet would be the weapon.

Cyberterrorism

Like terrorism, cyberterrorism has no accepted domestic or international definition (Boys, 2018; Klein, 2015; Marsili, 2019). Scholars debate whether or not cyberterrorism specific research should simply be incorporated into cybercrime studies (Albahar, 2019; Boys, 2018). Nonetheless, cyberterrorism is generally defined as terrorism in cyberspace that features attacks against computers and networks by subnational groups or individuals through violence or fear to coerce or intimidate a state's government or citizens to further political or social objectives (Jenkins & Godges, 2011; Klein, 2015; Marsili, 2019; Warf & Fekete, 2016). Terrorists realize the many advantages that can be gained in cyberspace and seek to exploit the dimension for their own advantage.

Cyberterrorism is inexpensive considering a computer and an internet connection is all that is typically required (Klein, 2015). The 9/11 Commission Report stated that al Qaeda spent between $300,000 to $400,000 USD in total to carry out their four separate attacks on September 11, 2001 (National Commission of Terrorist Attacks upon the United States, 2004). Yet, a cyberattack of comparable caliber could be even cheaper and would negate all logistical obstacles making it feasible for a cyberterrorist to conduct a devastating attack within the United States from anywhere in the world (Albahar, 2019).

Cyberterrorism is also more anonymous than conventional terrorism given the problems of attribution following a geographically separated cyberattack (Klein, 2015). Governments and private organizations can generally identify the source of cyberattacks to a large degree of certainty. However, any government counterattack would require indisputable evidence which is often difficult to produce (Tehrani, 2017).

The United States often publicly condemns Chinese hacking, has protested Russian interference in the 2016 U.S. presidential election, and has blamed North Korea for their Sony Pictures Entertainment cyber infiltration (Schulzke, 2018). Yet, officials in each of these countries have denied any involvement, calling the accusations groundless and false justifications for U.S. sanctions (Schulzke, 2018). It is relatively easy to decipher the source of a kinetic attack but cyberattack evidence varies (Schulzke, 2018).

There are a far greater number of viable cyberspace targets than tangible ones since cyberattacks render location and physical security irrelevant (Klein, 2015). It is therefore not out of the question for cyberterrorists to strike at the core of any large country or corporation displaying the most formidable physical defenses. Still, no terrorist group has successfully conducted a large-scale cyberterrorism attack against the United States as of 2020, but terrorists have made great strides exploiting the internet to facilitate communication, fundraising, propaganda, radicalization, and recruiting (Albahar, 2019; Dinniss, 2018; Fidler, 2016). Nevertheless, computer-assisted crime does not alone constitute cyberterrorism which is also distinct from cyberwarfare (Tehrani, 2017).

Cybercrime and cyberterrorism both involve illegal activities in cyberspace, yet they have different motivations and are therefore defined differently (Tehrani, 2017). Cybercrimes are broadly defined crimes committed by cybercriminals through information technology with no political or social motivations (Tehrani, 2017). Cyberterrorists, on the other hand, conduct cyberattacks using similar or identical methods to cybercriminals but with more violent and long-term political objectives (Dinniss, 2018). Further, non-violent cybercrimes committed for political purposes, are generally considered acts of *hacktivism*, or hacking for political activism (Klein, 2015). These hacktivists cannot be succinctly defined as cybercriminals or cyberterrorists and operate either independently or through state direction. Lastly, cyberterrorism is also different from cyberwarfare in that the main objective of cyberterrorism is to cause fear and harm while cyberwarfare focuses on more specific objectives encompassing non-conventional military attacks (Tehrani, 2017).

International Preparation

Despite ongoing concerns, international law does not directly address cyberterrorism since the lack of cyberattacks from terrorist organizations offers little incentive to draft such legislation (Baram & Menashri, 2019; Fidler, 2016). Creating international law related to cyberterrorism would be complex given the range of legal issues involved with the terms *terrorism* and *cyber* and by the inclusion of rapidly evolving technological advancements (Baram & Menashri, 2019; Boeke & Broeders, 2018; Fidler, 2016). It is also not clear how the Geneva Conventions and the greater laws of armed conflict apply to cyberterrorism (Marsili, 2019).

Laws regarding humane treatment in armed conflict are dictated in Common Articles 2 and 3 of the Geneva Conventions (Marsili, 2019). Specifically, Common Article 2 applies to international conflict between states and Common Article 3 applies to all forms of non-international conflict (Marsili, 2019). The self-defense statutes of Article 51 of the UN Charter and Article 5 of NATO could both apply if a destructive cyberattack comparable to a conventional attack occurred. However, international cyberwarfare conducted by non-state actors, such as cyberterrorists, does not fit neatly in the Geneva Conventions since Common Article 2 applies only to state conflict and Common Article 3 applies only to non-international conflict (Marsili, 2019). Therefore, there is no common article directly addressing international conflict by non-state actors which gives individual states discretion on how to apply elements of the Geneva Conventions; such as how the United States currently characterizes unlawful enemy combatants in the country's current *War on Terrorism*.

United States' Preparation

Attacks against U.S. infrastructure are not uncommon, but none have qualified as cyberterrorism as of 2020 (Klein, 2015). However, criminals continue to sell increasingly destructive black-market hacking tools and terrorist organizations are successfully achieving goals through cyber means making cyberterrorism attacks more probable (Klein, 2015; Nye, 2017). The United States has no domestic laws relating to a large-scale cyberterrorism attack thereby forcing the country to prosecute cyberterrorists using existing cybercrime or terrorism legislation (Tehrani, 2017). Domestic cyberterrorists would likely be tried through domestic law, but the issue becomes more complicated for international cyberterrorists.

The United States could deem transnational cyberterrorism attacks as cybercrimes under U.S. Code, Title 18, section 1030 *Fraud and Related Activity in Connection with Computers* (Tehrani, 2017). In this case, the United States could extradite offenders for domestic trials or apply extraterritorial jurisdiction to try cyberterrorists *in absentia*. The maximum fine for section 1030 offenses is 20 years imprisonment, though damage causing death would fall under section 225 of the Homeland Security Act amending section 1030 to authorize a lifetime sentence (Tehrani, 2017). Additionally, the Patriot Act discusses cyberterrorism in section 814. However, this section only relates to computer fraud offensives and would not be applicable to a large-scale cyberterrorism attack (Podgor, 2002). The United States could also declare international perpetrators of a destructive cyberterrorist attack terrorists. Assuming civilian deaths, these individuals would likely be accused of war crimes and be tried through military tribunals as unlawful enemy combatants. U.S. cyberterrorism legislation is incomplete, yet the country is not ignorant to the dangers of cyberterrorism.

Domestic Concerns. Many critical infrastructure control systems are susceptible to cyberterrorist attacks since the systems' complexities make eliminating all weaknesses virtually impossible (Klein, 2015). In 2012 then U.S. Secretary of Defense Leon Panetta warned that the United States was becoming increasingly vulnerable to extremist attacks that could harm the country's financial networks, transportation systems, and power grids

(Naím, 2017; Nye, 2017). Further, in 2013 the Department of Defense's Science Board stated that the country should not assume that critical systems can be defended from a well-resourced cyberattack (Mazanec, 2016). In 2014 then Director of National Intelligence, James Clapper, even ranked cyber threats above terrorism as the top U.S. security risk (Tabansky, 2018). Realizing these vulnerabilities, in 2015 the Department of Defense began crafting a cyber deterrence strategy that greatly expanded offensive capabilities (Osawa, 2017; Wilner, 2020). Still, in 2016 Mr. Clapper stated that evolving cyber capabilities were outpacing a common understanding of its norms of behavior which could increase the chances of misunderstandings and lead to unintentional escalation (Mazanec, 2016). The Defense Science Board also reaffirmed their position in 2017 stating that offensive cyber capabilities of potential adversaries will likely far exceed the United States' ability to defend them for the next five to ten years (Wilner, 2020).

Deterrence

History continues to witness the evolution of warfare. New technologies forge innovative offensive weapons that are immensely successful at first until comparable deterrence is created through like modernization and policy. Deterrence typically involves the threat of punishment through retaliation and works best against rational and predictable adversaries (Wilner, 2020). U.S. deterrence has significantly evolved since 2003 and currently focuses on near-peer adversaries, rogue and weak states possessing limited weapons of mass destruction, and violent non-state actors (Wilner, 2020). Yet, cyber deterrence on an international level can be complex and must draw from elements of national security, international crime, espionage, and international conflict (Matwyshyn, 2018; Wilner, 2020).

Joseph Nye lists the four factors of cyberspace deterrence as the threat of retaliation, denial, fear of entanglement, and norms (Nye, 2017; Shad, 2018). Attribution is the main barrier to cyber retaliation needed for deterrence by punishment since it is often difficult to identify both the attacker and the source of the cyberattack (Hodgkinson, 2018; Nye, 2017; Shad, 2018). Deterrence by denial is best realized when a state has a resilient cyber defense capable of preventing or quickly recovering from a cyberattack (Nye, 2017; Shad, 2018). Entanglement deterrence is supported through international agreements such as the Budapest Convention and by international organizations such as NATO (Shad, 2018). Lastly, norms work by naming and undermining perpetrators of cyberattacks (Shad, 2018). U.S. cyber deterrence policy has shifted from denial under President Bush to a punishment approach under President Obama and President Trump. The United States regularly reviews cyber deterrence options against non-state actors and evaluates ways to deter Russia, China, North Korea, and Iran from conducting cyberattacks against the country (Klein, 2015). However, the number of cyberattacks aimed at U.S. targets has steadily risen for the past 15 years (Wilner, 2020).

State and non-state actors have infiltrated U.S. systems and caused damage and theft without crossing the government's threshold for escalation or retaliation short of sanctions (Bracken, 2017). These attacks, then, could either be viewed as a failure of deterrence or falling into the *gray zone* between war and peace (Nye, 2017). The United States is particularly at a disadvantage compared to cyberterrorists and authoritarian regimes since these organizations are not bound by legal or political constraints (Mazanec, 2016; Naím, 2017). An asymmetry also exists in that weak, rogue, or non-state actors with limited cyber platforms have the least to lose and the most to gain from cyber conflict (Wilner, 2020).

Enforcement

German philosopher Immanuel Kant wrongly concluded in the late 1700s that states would eventually seek peace through international governance due to the ever-increasing violence of war (Barrett, 2017). However, international governance has yet to materialize and existing transnational organizations are not completely in sync with evolving threats. In practice, states prefer to preserve their relative power by conducting actions that fall under the threshold for conflict (Barrett, 2017). Challenges that must be overcome to increase international agreement on cyber cooperation are trust, perceptions, and state sovereignty (Baram & Menashri, 2019). There is nearly international consensus that cyberattacks could be considered *acts of war* depending on the circumstances and that *proportionality* permits conventional retaliation to cyberattacks (Hodgkinson, 2018). Relating cyberattacks to acts of war should encourage states to create robust self-defense plans to prevent such attacks. Yet, cyber self-defense is still a new and evolving topic.

There are currently no domestic or international laws addressing self-defense in cyberspace (Cook, 2018). However, in 2003 the United States published *The Strategy to Secure Cyberspace* which implies that the country reserves the right to respond to a cyberattack through kinetic or non-kinetic actions (Klein, 2015). Also, President Obama’s 2011 *International Strategy for Cyberspace* stated that the United States will use all necessary means for cyberattack defense but will limit military force as a last resort (Mazanec, 2016; Wilner, 2020). Because of this, the United States has a wide variety of retaliatory options available including conventional options authorized solely by the president under the Authorization for Use of Military Force (Marsili, 2019). In 2012 the U.S. government stated that a cyberattack could be viewed as an armed attack implying that the country could come to the defense of other states in accordance with Article 51 of the UN Charter or Article 5 of NATO (Hodgkinson, 2018; Klein, 2015).

Additionally, for the first time in February 2016 the United States began conducting open offensive military cyberattacks against ISIS to augment ongoing conventional operations (Fidler, 2016; Hatch, 2018). The nature of these attacks remains classified but U.S. Cyber Command targeted the terrorist organization's ability to spread propaganda, recruit, and control operations in Iraq and Syria (Fidler, 2016). The United States claimed that its actions were in accordance with international law given that domestic cyber doctrine states that all actions must conform to U.S. laws and regulations while being cognizant of international law (Brantly, 2016; Fidler, 2016). The U.S. military has demonstrated that active cyber operations can be effective. However, this expertise has not yet transitioned to U.S. private businesses including operators of U.S. critical infrastructure.

The preferred universal method of cybersecurity involves passive defense measures such as anti-virus software and intrusion detection systems (Van Dine, 2020). Yet, the overwhelmingly high number of successful cyberattacks suggests that passive defense security measures could be improved (Van Dine, 2020). However, active cyber defense operations conducted by private U.S. corporations is currently considered illegal without consent which also generally correlates with the Budapest Convention's interpretation of the issue (Cook, 2018; Van Dine, 2020). Active cyber-defense measures would also likely be in violation of the U.S. Computer Fraud and Abuse Act that prohibits accessing computers without authorization to obtain information, transmit code, or cause damage (Cook, 2018).

However, members of the U.S. government are attempting to expand the cyber powers of private industry. In 2019 Representative Tom Graves introduced a congressional bill for the Cyber Defense Certainty Act that would grant authority for private organizations to infiltrate the networks of their cyber attackers (*H.R.3270 - Active Cyber Defense Certainty Act*, n.d.). This Act would let private companies loiter in foreign networks to identity their attackers and discover their methods which is known as *hacking back* (Cook, 2018). Hacking back is part of active cyber defense which encompasses operating inside and outside of defenders' networks to discover and degrade aggressor capabilities (Cook, 2018; Van Dine, 2020).

In absence of active cyber defense measures for private U.S. industry, many feel that public and private sector cybersecurity matters should not be siloed since a breach in either could affect both (Healey, 2018; Matwyshyn, 2018). However, some critical infrastructure components, such as air traffic control systems and nuclear power plants, already encompass both public and private sector security elements known as *reciprocal security vulnerability* (Matwyshyn, 2018). The private sector has also worked with government organizations on a range of cyber related issues through public-private partnerships created in 1998 by President Clinton's Presidential Decision Directive 63 (Healey, 2018). Additionally, the Cybersecurity Act of 2015 provides a framework for public and private sectors to cooperate with the intent of working toward the common goal of cybersecurity through voluntary information sharing (Kosseff, 2018; Matwyshyn, 2018). Expanding active cyber defense into the U.S. private sector could bolster critical infrastructure cybersecurity and reduce the number of successful cyberattacks through measures such as hacking back and information synthesis between the public and private sectors. However, some feel that no amount of preparation can deter a cyberterrorism attack against the United States.

Counterarguments

A majority of cyberterrorism literature focuses on preparation and deterrence through the direction of domestic and international laws, but other aspects suggest that the United States will always be vulnerable to asymmetric cyberattacks (Klein, 2015). This literature indicates that cyberattacks against U.S. public and private information technologies is a daily occurrence and the government subsequently conducts little to no public responses since a vast majority of the attacks are unsuccessful (Klein, 2015). Additional counterarguments believe that cyberterrorists motivated by ideology based on religion or factionalism that embraces death are not concerned with repercussions and may be undeterrable (Klein, 2015). It would also be very difficult to create proportional and creditable deterrence options against adversaries will high risk tolerances (Klein, 2015). Additionally, choosing military targets following a cyberterrorism attack from a non-state actor could be problematic since terrorists are not bound by geographical borders and largely operate amongst civilians (Klein, 2015). The final counterargument is that terrorists might even exploit any law or proportional response plan to their advantage since they would already know the methodologies of their targets (Klein, 2015). State-focused cyber deterrence against North Korea, Russia, and China is also occasionally discouraged.

North Korea became a nuclear power in 2006 to presumably counter the comparatively superior military power of the United States (Bracken, 2017). At the opposite end of the spectrum, the country is also advancing their cyber capabilities (Bracken, 2017). Some scholars believe that if North Korea had the ability to launch a decisive large-scale cyberattack against United States, they would likely still refrain since the cyberattack could easily be countered with a conventional military response from the United States and potentially create a conflict that North Korea could not win (Bracken, 2017). Additionally, China and Russia have successfully gained territory in the South China Sea and in Ukraine and Crimea, respectively, by operating under the threshold for triggering U.S. and international reactions which they have a practice of doing in all actions including in cyberspace (Bracken, 2017). These two countries would fare better than North Korea in a conventional war with the United States, but a deadly war would also not be in their national interests (Bracken, 2017).

The 20th century was defined by conventional wars, whereas the 21st century has so far been dominated by asymmetric hostilities including terrorism and cyber threats. Countless examples of failed deterrence initiatives exist throughout history which will continue into the future against a multitude of seen and unexpected adversaries. When deterrence fails, having deliberate response plans could increase the chances of successful retaliation while mitigating escalation. Adversaries might also be deterred from aggression after examining an unpalatable but pending response. However, announcing what cyberattacks would warrant military responses could allow adversaries to design attacks just short of the kinetic response threshold.

Summary

The rules of war have been discussed for thousands of years but integrating *cyber* and *terrorism* into the discussion has only recently begun following the invention of the internet and following the 9/11 attacks. It is improbable that terrorism and cyberwarfare will be conceptually defined at the international level any time soon since it is unlikely that states will conclusively agree to alter existing regulations. Most states will therefore continue to act in accordance with domestic doctrine imbedded in their own ideologies to the frustration of others.

Currently, no country can assume victory against the U.S. military which drives asymmetric developments for potential U.S. adversaries including cyberspace operations and state-sponsored terrorism. Additionally, terrorist organizations continue to search for all conceivable ways to gain advantages against much more powerful adversaries. Because of this, cyberterrorism is developing as a dangerous new threat that has possibly been inadequately addressed due to reasons outlined using the punctuated equilibrium theory.

It is also unclear how the United States would react to a successful damaging cyberterrorism attack against the country. The United States could respond to these attacks in a variety of ways through military or diplomatic channels using overt or covert methods and by means of kinetic or non-kinetic actions. Therefore, more cyberterrorism deterrence and response research might be needed to avoid reactionary decisions made in an emotionally charged environment following a successful destructive cyberterrorism attack.

In Chapter 2, I provided a summary of literature on all available information concerning the development of the cyber domain and terrorism, and the U.S. and international attitudes toward them. I also gave examples of how states have been nefariously using cyberspace to their advantages and highlighted ambiguities in domestic and international legislation related to the subjects. I finally identified a gap in literature concerning the lack of cyberterrorism response guidelines and addressed why the United States might need to preemptively draft cyberterrorism deterrence and response guidelines. I introduce the research design and approach for the study in Chapter 3.

Chapter 3: Research Method

Introduction

The purpose of this qualitative study was to explore the perceptions of terrorism and cybersecurity experts to understand how the United States might better prevent and respond to large-scale cyberterrorism attacks. A major successful cyberterrorism attack has never been conducted against the United States so it remains unseen what guidelines the country will use as the basis for a response. The current lack of guidance could leave the United States in a vulnerable position following a successful large-scale cyberterrorism attack given the unpredictability of potential responses. Through expert interviews, I addressed whether current policies were adequate to respond to large-scale cyberterrorism attacks, or if additional cyberterrorism specific policies should be created to ensure preemptive and palatable options. In Chapter 3, I discuss the research design of the study, the rationale for the design, and the role of the researcher. I also explain the study's methodology including participant selection, instrumentation, and data collection and analysis. I finally discuss issues of trustworthiness and ethical procedures.

Research Design and Rationale

Research Question: How do terrorism and cybersecurity experts perceive that the United States might better prevent, cope with, and respond to large-scale cyberterrorism attacks?

I chose a qualitative research design for this study. Creswell (2013) explained that qualitative research is used to explore a problem through variables identified as a result of direct communication with participants. The focus of this qualitative study was the exploration of the perceptions of U.S. terrorism and cybersecurity experts to better understand how the country might better prevent and respond to large-scale cyberterrorism attacks. The rationale for this approach was to give these experts latitude to describe in their own words the applicability of better deterrence and response guidelines for a large-scale cyberterrorism attack. I therefore collected data through semistructured one-on-one telephone interviews. I asked open-ended questions in the same order to all participants with the addition of follow-up and probing questions as required to insure full answers to all questions.

Role of the Researcher

As the researcher, I was involved in all aspects of this study. I initially identified the area of study based on my personal interests and determined that a gap in literature existed through an exhaustive literature search. I then identified the study's topic, conducted a literature review to incorporate all known information on the topic, and purposefully selected knowledgeable participants with whom I had no previous affiliations. It was paramount that I identified potential biases and remained cognizant of them throughout all aspects of the study to uphold the integrity of the research.

I was the sole instrument in the qualitative data collection process. I collected data from in-depth, semistructured telephone interviews which I organized, analyzed, and interpreted. Interview participation was voluntary, and I posed interview questions in a neutral manner as part of an unbiased interview process. I had no personal or professional affiliations with any participants, but I have lived the effects of 9/11 as a military member for 15 years and therefore used bracketing strategies to address any inherent biases gained through previous military experiences as well as to suspend any personal views acquired through the literature review and data collection. I lastly complied with all guidelines outlined in Walden University's Institutional Review Board (IRB) for ethical research.

Methodology

Participant Selection

After IRB approval, I sent prospective participants study invitations through individual e-mail or LinkedIn messages explaining the study and selection criteria. Participants in this study are experts in their respective government, security, or educational career fields. Targeted participants demonstrated familiarity in the study's topic by previously relating their expertise to aspects of cyberterrorism. For the purposes of this study, I defined an expert as an individual who has worked professionally in two or all three cyber, terrorism, and national security career fields within the federal government for at least 10 years since 2001. The timespan justification was to ensure that participants had been active in their respective occupations since 9/11 and had practiced their profession over the course of at least two presidencies.

I identified 89 potential participants meeting expert criteria from a multitude of professions including government officials, professors, lawyers, cybersecurity members, and scholars to align with the research question's focus on the perception of experts. Of these participants, 79% have federal government work experience, 58% hold doctoral degrees, and 61% and 45% are cyber and terrorism professionals, respectively. I did not identify participants by name in this study and I also did not include individual names in transcripts of recorded interviews. I received positive responses from nine participants. Themes began to emerge after the first three interviews and data saturation was firmly established after the completion of the ninth and final interview.

Instrumentation

The instrument for this study was a one-on-one semistructured telephone interview. I chose semistructured interviews to allow leeway for script diversions for clarifications or to grasp deeper meanings to answers. I pilot-tested interview questions with three volunteer peers familiar with aspects of cyberterrorism before conducting interviews with actual participants. I recruited volunteers from friends and co-workers who were familiar with the study's topic. I refined my interview questions and delivery through the pilot study. Each interview, while not identical, followed the interview protocol in Appendix A which includes the interview questions in Appendix B. I asked follow-up questions for any clarifications and to probe for a deeper understanding of participant responses. The interviews took between approximately 20 to 60 minutes to complete and averaged 38 minutes each. No follow-up procedures or follow-on interviews with the participants were required.

Procedures for Data Collection

I collected data from nine experts over a 6-week interview period from August 27 to October 3, 2020. Before beginning each interview, I established rapport with the participant by introducing myself, discussing my background, explaining the goals and objectives of the study, and clarifying that all shared information would remain confidential. The participants all agreed to an informed consent which was confirmed in the interview protocol before each interview. Audio interview recordings were transcribed to Microsoft Word and compared for accuracy. I then sent the transcribed recordings to the participants to confirm the accuracy and to allow them to make changes or add additional comments. The audio recordings were deleted after each participant approved their transcription. Finally, I sent an Executive Study to each participant after completion of the study along with a personalized thank you message before ceasing communication.

Data Analysis Plan

Qualitative analysis converts data into findings after making sense of the large quantity of data (Patton, 2015). Data analysis began after each transcript was reviewed and returned by the participant, or after one week of no response. I linked the data collected from the interviews to the research question and theoretical framework using the qualitative data analysis software NVivo to identify patterns and themes.

The qualitative NVivo program is used to classify, sort, arrange, and compare data. Using NVivo, I coded the interview data through predetermined codes and emerging codes in order to extract ideas and categories for comparison and analysis. I then exhaustively study all coded NVivo data to interpret categories and themes in order to draw conclusions.

Data analysis ran concurrently with data collection during first-cycle coding to complement the predetermined codes formed through the literature review. A robust data management plan ensured that data were not mismanaged through proper organization and storage. I initially hand coded the interview data to gain a deeper understanding of the data as well as to identify predetermined codes and conceptualize emerging codes. I then used NVivo to extract emergent codes and finally formulated all collected data into themes at the completion of second-cycle coding to complete data aggregation.

Issues of Trustworthiness

I interacted with all study participants in accordance with IRB guidelines. I obtained IRB permission to conduct research before data collection began. I handled the data purposefully throughout the data collection process. I used a transcription service called TranscribeMe to transpose audio recordings into verbatim Microsoft Word documents which I then compared to the audio recordings for accuracy. All TranscribeMe employees sign non-disclosure agreements to keep transcribed data confidential. I deleted audio recordings after the participants approved the transcripts, and I secured printed transcripts in a personal safe until the completion of the study after which I destroyed them. Lastly, electronic copies of transcripts and data will be kept on a password protected hard drive in a safe for five years before also being destroyed.

Ethical Procedures

I treated all participants with the upmost respect. I initially contacted participants through e-mail or LinkedIn messages and conducted all subsequent contact through private phone conversations or personal e-mail correspondence. I ensured participants agreed to an informed consent before conducting each interview. The consent form explained that participation was voluntary and could be stopped at any time. The form also explained the reasoning for the study and the methods used throughout the study. It lastly stated that personal information of each participant would be kept confidential.

Summary

This chapter presented the research design for a qualitative study on the applicability of improved deterrence and response guidelines for a large-scale cyberterrorism attack. I served as the primary research instrument and gathered data through semistructured telephone interviews. Nine participants were interviewed over a 6-week period. I extracted data from interview transcripts and subsequently coded and analyzed the data to draw conclusions using NVivo software. I took thorough care to ensure participants remained anonymous by properly securing data, and that all ethical standards were followed in accordance with IRB guidelines. I present the findings of this research in Chapter 4.

Chapter 4: Results

Introduction

The purpose of this qualitative study was to explore the perceptions of experts to better understand how the United States might better prevent and respond to large-scale cyberterrorism attacks. A major successful cyberterrorism attack has never been conducted against the United States, so it remains unseen what guidelines the country will use as the basis for a response. The current lack of guidance could leave the United States in a vulnerable position following a successful large-scale cyberterrorism attack given the unpredictability of potential responses. Through expert interviews, I addressed whether current policies are adequate to address large-scale cyberterrorism attack preparation and response guidelines, or if additional cyberterrorism specific policies should be created to ensure preemptive and palatable options.

A single research question guided this study: How do terrorism and cybersecurity experts perceive that the United States might better prevent, cope with, and respond to large-scale cyberterrorism attacks? One hundred and twelve peer-reviewed articles supported the findings of this study. A detailed literature review of all publicly available information related to cyberterrorism confirmed that the U.S. government has not openly considered prevention and response strategies for a large-scale terrorism attack. The scope of this study was nationwide, and 89 potential participants meeting expert criteria were contacted after IRB approval. Positive responses were received from nine experts which was slightly less than the predicted 11 responses calculated using an eight to one response rate.

I pilot-tested interview questions with three volunteer peers familiar with aspects of cyberterrorism from August 25–26, 2020 after IRB approval (08-24-20-0531149) but before conducting interviews with actual participants. I refined my interview questions and delivery through the pilot study, but I made no changes to data analysis strategies. The nine participants were then interviewed over a 6-week period from August 27 to October 3, 2020.

In Chapter 4, I discuss the results obtained from the analysis of primary data gathered through semistructured telephone interviews. This chapter begins with the setting and demographics. I then give a detailed description of the coding strategies used for data collection and data analysis before concluding with evidence of trustworthiness and the major themes cultivated from data analysis.

Study Setting

I conducted semistructured telephone interviews at a date and time of the participants' choosing in order to give them the opportunity to identify a comfortable setting where they could respond fully and freely without time restrictions. All participants chose weekdays during normal work hours. I also recorded the interviews in various private and secluded settings with strong mobile phone and internet reception. All interviews were therefore completed with no distractions, interruptions, or time constraints as confirmed by a review of the verbatim transcripts. The participants did not identify any personal or organizational commitments that would have influenced them at the time of this study.

Demographics

Participant criteria for this study included experts who have worked professionally in two or all three cyber, terrorism, and national security career fields within the federal government for at least 10 years since September 2001. The timespan justification was to ensure that participants were active in their respective occupations since 9/11 and have practiced their profession over the course of at least two presidencies. I gathered data from nine experts with past federal government experience and with 138 and 72 years of cumulative cyber and terrorism experience, respectively. Demographics such as age, race, religion, and gender were not considered relevant to answering the research question. Applicable participant demographics are listed in Table 1.

Table 1

Demographics of Participants

Participant ID	Education level	Years of experience cyber	Years of experience terrorism	Fed govt experience	Present profession
E1	Doctorate	0	12	Yes	Professor
B2	Doctorate	14	40	Yes	Consultant
P3	Doctorate	13	0	Yes	Cybersecurity
C4	Doctorate	20	0	Yes	Cybersecurity
T5	Doctorate	21	0	Yes	Military
J6	Doctorate	6	12	Yes	Professor
A7	Masters	0	5	Yes	Researcher
T8	Doctorate	35	3	Yes	Professor
P9	Doctorate	29	0	Yes	Government

Data Collection

Walden University granted IRB approval for this study on August 24, 2020 with approval number 08-24-20-0531149. Following this approval, I sent invitation letters to 89 potential participants through individual e-mail and LinkedIn messages and received responses until September 17, 2020. I collected data from nine participants using semistructured telephone interviews from August 27 to October 3, 2020. I asked clarifying questions propagated from participant answers to the semistructured interview questions located in Appendix B in order to gain a complete understanding of each answer as well as to explore deeper meanings to answers. The interviews ranged from 20 to 61 minutes, averaged 38 minutes, and totaled 5 hours and 48 minutes. I recorded each interview on a digital voice recorder which I then downloaded to a password protected external hard drive. I secured this hard drive in a personal safe when not in use. I had the recordings transcribed verbatim to Microsoft Word using the transcription service TranscribeMe which yielded 108 pages of transcriptions. I compared the recordings to each transcription to ensure accuracy before deleting the recordings. I then sent the transcriptions to the participants to make any changes they felt necessary. Only one participant responded with edits. Data collection went as planned and no unusual circumstances were encountered. Individual interview details are described in Table 2.

Table 2

Interview Statistics

Participant ID	Date of interview	Duration (h.m.s)	Transcribed pages
E1	27 Aug 20	0.41.52	12
B2	28 Aug 20	1.01.42	15
P3	28 Aug 20	0.35.14	13
C4	03 Sep 30	0.48.43	15
T5	11 Sep 20	0.47.17	13
J6	29 Sep 20	0.28.39	12
A7	30 Sep 20	0.26.32	9
T8	02 Oct 20	0.20.01	7
P9	03 Oct 20	0.38.08	13

Data Analysis

Participant transcriptions were exported into NVivo software which I used as a data analysis aid. I then subsequently coded the transcriptions to highlight patterns in the data to generate categories which were analyzed for connections. Saldaña (2016) explained that qualitative data coding involves dividing, grouping, reorganizing, and linking codes in order to search for meanings and to develop explanations. Coding for this study was an iterative process that utilized both precodes and emergent codes. I incorporated a variety of coding methods selected to best synthesize data throughout the coding process.

I formed precodes during literature review which I chose based on the study's research question, framework, and approach. I used the *structural coding* method for precodes which resembled broad topics gathered for the purpose of more detailed analysis (Saldaña, 2016). I reviewed all transcripts exclusively for precodes before emergent codes were identified. The precode list was based on the interview questions and comprised of the following codes: *awareness alignment*, *common understanding*, *cyberattack probability*, *cyberattack understanding*, *decision-maker priorities*, *international law*, *national security priorities*, *policy issue drivers*, *policymaker perceptions*, *possible responses*, *precautionary measures*, and *U.S. preparations*. Precodes allowed me to loosely sort the data by research question in order to approach the data from another perspective.

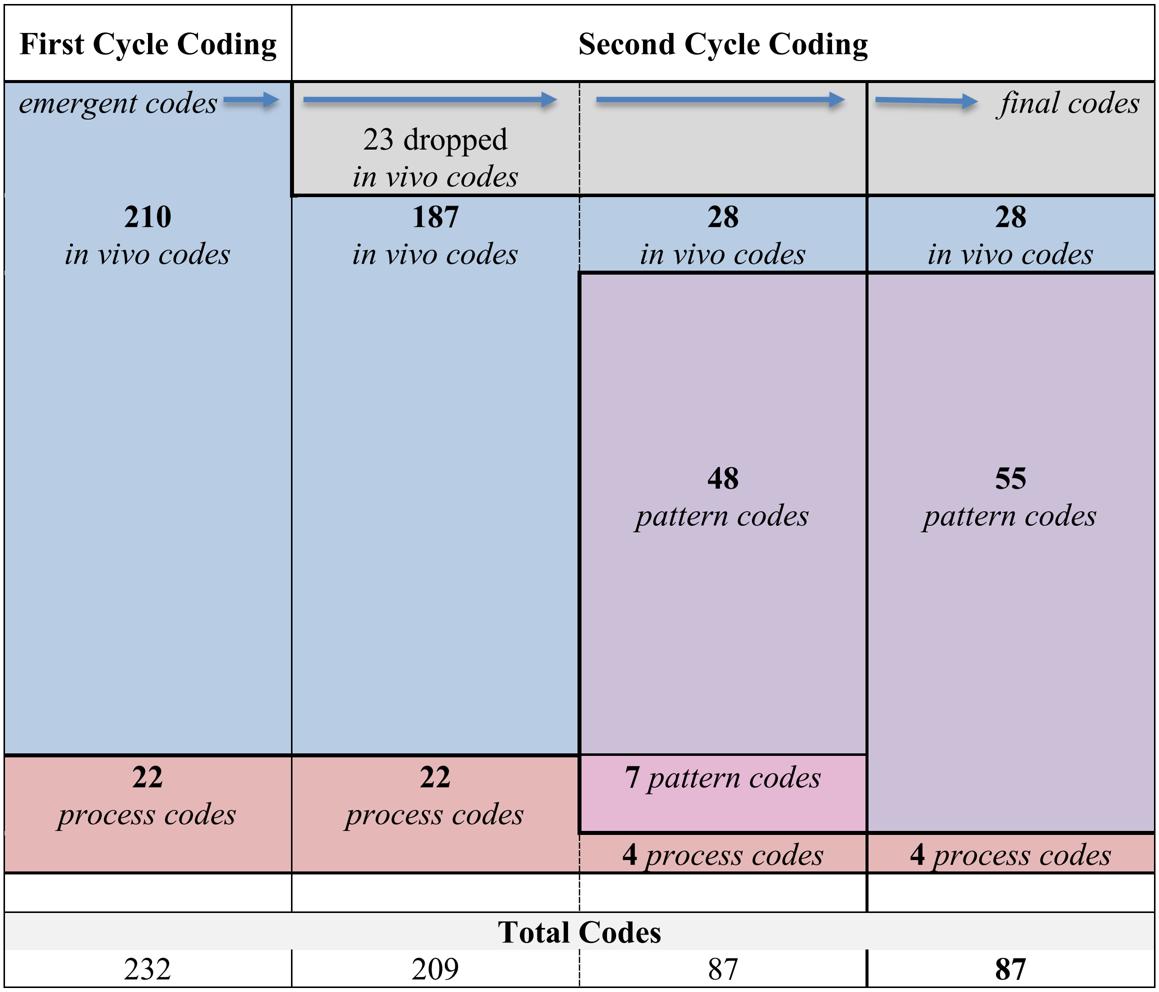
I then identified emergent codes through coding and recoding in both first and second-cycle coding. Saldaña (2016) explained that first-cycle coding is initial coding that is used as a baseline to see what direction the study will take. I incorporated *in vivo* and *process coding* methods in first-cycle coding. In vivo codes, or verbatim codes, are generated from the actual language of participants and are identified by quotation marks. Process coding focuses on the changing and repetition of action as well as the disruptions that occur within human goal setting or problem-solving interactions and are identified with gerunds (Saldaña, 2016). I used the process coding method judiciously in this study for coding punctuated equilibrium theory related participant responses.

I recoded the transcripts using first-cycle coding methods to ensure that all emergent codes were applied throughout each transcript. First-cycle in vivo and process coding generated 232 emergent codes. I then used second-cycle coding to reorganize and reanalyze data gathered through first-cycle coding methods. Here, I predominately used *pattern coding* which condensed codes into a smaller number of categories by merging codes together while dropping others. Saldaña (2016) recommended 50 to 100 total codes, 15 to 20 categories, and five to seven major themes. Data analysis for this study produced results similar to Saldaña's recommendation with 87 total codes grouped into 11 categories and six major themes.

First and second cycle coding development is illustrated in Figure 1. The study's themes, categories, and respective code sums are presented in Appendix C which also lists amplifying information of all 87 second cycle codes including participant contributions, interview questions utilized, and associated first cycle code frequencies.

Figure 1

Code Development



First Cycle Coding	**Second Cycle Coding**		
emergent codes →	→ 23 dropped *in vivo codes*	→	→ *final codes*
210 *in vivo codes*	**187** *in vivo codes*	**28** *in vivo codes*	**28** *in vivo codes*
		48 *pattern codes*	**55** *pattern codes*
22 *process codes*	**22** *process codes*	**7** *pattern codes*	
		4 *process codes*	**4** *process codes*
Total Codes			
232	209	87	**87**

Discrepant Cases

Two discrepant cases involving one participant emerged from the study. This participant believed that terrorists do not need state assistance to conduct a large-scale cyberterrorism attack and also believed that a large-scale cyberterrorism attack was likely in the near future. Six other participants disagreed with this assessment and felt that state assistance is required to conduct a large-scale cyberterrorism attack although any attack is unlikely. The divergent participant contributed to data saturation in all other areas despite deviating from the majority in the identified discrepant cases.

Evidence of Trustworthiness

I achieved trustworthiness of this study through acknowledging discrepant cases as well as through credibility, transferability, dependability, and confirmability.

Credibility

Credibility in a qualitative study relates to the degree that the results reflect the experiences of the participants. To facilitate open and honest responses, I ensured that participants were aware that no identifying information would be used in the study and that they could opt out at any stage. I also ensured that all data were creditable by comparing each transcription to its audio recording for complete accuracy. I then sent the transcriptions to the participants to review and edit before using the final transcriptions for data analysis. Additionally, each potential participant went through multiple iterations of scrutiny before being included in the final list of 89 experts which resulted in the elimination of 61 individuals from the original 150-member list.

Transferability

Transferability of this study is possible since I described in detail the rationale, structure, and justification of the study, as well as participant demographics. While the participants were not directly identified in this study, I provided sufficient detail to highlight their levels of expertise. Cyberterrorism and U.S. interventions are respectively global and nationwide by definition. The transferability of this study is therefore possible to a multitude of government, cyber, and terrorism focused organizations throughout the world.

Dependability

I ensured the dependability of this study by aligning the research question to the study's problem and purpose. I also derived the interview questions from the purpose of the study while considering the study's theoretical foundation. Additionally, I conducted an exhaustive literature and located 112 predominately peer-reviewed journal articles using detailed search criteria in multiple databases. I also remained cognizant of the scope of the study through the iterative and thorough data analysis process.

Conformability

Lastly, conformability relates to the objectivity of the study. I was exclusively responsible for all data collection and analysis. I first collected data in an objective manner after identifying potential researcher biases and implemented bracketing techniques. I then coded data using precodes and emergent codes through primary and secondary cycle coding and recoding. This iterative coding process resulted in five coding revisions for each transcript to ensure that all data were objectively extracted.

Study Results

Six themes emerged from the data analysis relating to the study's single research question: How do terrorism and cybersecurity experts perceive that the United States might better prevent, cope with, and respond to large-scale cyberterrorism attacks? Five of the six themes contained two or more categories which resulted in 11 categories containing 87 total codes for the study as seen in Figure 2. A detailed code list is located in Appendix C.

Figure 2

Themes, Categories, and Codes

Themes	Categories	Codes
Terrorists’ Cyber Capabilities		6
Large-Scale Cyberterrorism Attack Probability	Low Probability	4
	Activity Below War Threshold	6
Large-Scale Cyberterrorism Attack Likely Responses	Attribution Considerations	6
	Lethal Response	2
Cyberterrorism Prevention Measures	Collective Coordination	17
	Preparation	15
Cyberterrorism Policy Agendas	Technical Knowledge	4
	Policymaker Consciousness	18
	Agenda Change Factors	3
International Cyberterrorism Considerations	International Law Validity	2
	International Law Integration	4

Data were generated from nine participants through 18 interview questions located in Appendix B. All interview questions were aligned with the research question by considering the study’s problem, purpose, structure, and theoretical foundation. The six themes generated from data analysis are as follows:

Theme 1: Terrorists’ Cyber Capabilities

The first theme that emerged was related to the current cyber capabilities of terrorist organizations. The literature review indicated that terrorist organizations are capable of successfully manipulating cyberspace to their advantages, and the study's research question suggested that terrorist groups are likewise capable of carrying out a large-scale cyberterrorism attack against the United States. Terrorist groups have long desired to gain capabilities in cyberspace which they continue to successfully pursue, yet most participants believed that terrorists currently do not possess the capability to conduct a large-scale cyberterrorism attack against the United States without state assistance. Given this, the discussion of a pending large-scale cyberterrorism attack is incomplete at present without the inclusion of states.

Participant J6 stated that terrorists are not yet able to produce kinetic-like effects through the cyber realm. Likewise, participant P9 felt that terrorist groups would need to hire out the capability to have a sustained effect over time in cyberspace since they lack the sophistication to do it on their own. Participant C4 stated that, "the organic capability is generally limited for international terror groups. They're digitally okay and not dumb, so they can serve as proxies for some of the major players: Russia, North Korea, China, and Iran among others." He also noted that they can still do damage with a radicalized insider.

Further, participants E1 and C4 felt that terrorists would need assistance from states to have any chance of successfully conducting a large-scale cyberterrorism attack against the United States, though there is no evidence that states are currently augmenting the cyber capabilities of terrorist organizations. Participant P3 highlighted that even the NotPetya attacks against Ukraine conducted by a state (Russia) were only effective for a few days, so it is unlikely that an even more sophisticated attack could be conducted by a non-state actor against any country with respectable cyber defenses.

However, participant B2 argued that terrorists could actually possess the capabilities to conduct an unassisted large-scale cyberterrorism attack against the United States since only a few smart people are needed to create a cyberattack mechanism. Yet, he did note that terrorist organizations do not need capability organic to their organization which "leaves the door open for a lot of potential mischief by terrorist organizations, whether they build their own capability, or they borrow it, or buy it from somebody else."

Theme 2: Large-Scale Cyberterrorism Attack Probability

Predictably, the six participants who felt that terrorist organizations lack the ability to unilaterally conduct large-scale cyberterrorism attacks also believed that such an attack against the United States is low. The exception is participant B2 who felt that the United States will fall victim to a successful large-scale cyberterrorism attack within the next few years. However, most participants still acknowledged that smaller scale cyberattacks are being conducted against the United States on a regular basis. The first category in this theme addresses the low probability of a large-scale cyberterrorism attack against the United States while the second category focuses on problematic cyber activities currently being conducted against the country.

Low Probability

Participant E1 was skeptical about the threat of a major cyberterrorism attack that might kill scores of U.S. citizens and instead views cyber as exclusively a state threat. Participant C4 also felt that a major cyberterrorism attack is unlikely and not nearly as realistic as “a death by a thousand cuts” which relates to the second category in this theme, *activity below war threshold*.

Activity Below War Threshold

Participant T5 stated that the United States is being attacked right now, but not to the level of 9/11, and from adversaries who are either attempting to cause disruption or are probing the U.S. cyber network. Similarly, participant E1 believed that terrorist organizations are intensely probing the United States in a multitude of ways, including testing the country’s critical infrastructure, while participant A7 felt that terrorists prefer to gather information through cyber means from vulnerable businesses to use for intimidation purposes. Lastly, participant C4 reiterated that most digitally connected organizations throughout the world who could help terrorist organizations would rather practice cyber espionage with the goal of having no reaction from the countries being probed. Because of this, he felt that aggressive offensive cyber actions against the United States are unlikely.

Participant B2 clarified that while cyber espionage needs to be addressed, it is not cyberterrorism but simply an extension of “old-fashioned spying” which is not illegal in international law. Yet, participant T8 is concerned that organizations have been conducting *intelligence preparation of the environment* with the intention of folding cyber into any future conflicts. Similarly, participant P9 explained that the United States is concerned with attacks generated from weaponizing capabilities gained from cyber espionage since these types of threats, such as national election interference, have the potential to undermine the very basis for democracy. However, participant E1 argued that the United States still does not know exactly how to respond to harmful attacks against the country that utilize only "zeros and ones." Participant C4 lastly felt that organizations can destabilize a country with ease if they conduct cyber operations just below the threshold of warfare since those operations do not galvanize citizens or gain the attention of policymakers.

Theme 3: Large-Scale Cyberterrorism Attack Likely Responses

Most participants felt that the United States will conduct a forceful and kinetic response to a successful large-scale cyberterrorism attack since the effects of both a large-scale cyberattack and a large-scale conventional attack would be similar. However, most participants also acknowledged that attribution must first be levied in a timely manner which is predictably much more difficult in the cyber realm. Given this, the first category in this theme is *attribution considerations*.

Attribution Considerations

Participants E1, J6, and T8 argued that the United States possesses the forensic abilities to very accurately attribute cyberattacks, and participants B2 and P9 felt that U.S. cyber attribution is improving but acknowledged that it still takes too long to lay blame. Participant J6 clarified that the U.S. government is often reluctant to revel attribution sources since he likened this action to "blowing a human asset conducting a covert operation." Participant B2 further clarified that it is easy for countries to disguise attacks, such as Russia routing cyberattacks through China, which could hinder the attribution process. Lastly, participant P3 explained that most private companies are actually not concerned with attribution since their focus is on stopping the cyberattack, minimizing the event, and preventing future vulnerabilities. He clarified that private companies cannot conduct offensive cyber operations, so they are not concerned with identifying their attackers which minimizes offensive private sector cyber innovation. The second category in this theme is *lethal response*.

Lethal Response

Despite attribution difficulties, most participants agreed that the United States would respond quickly, aggressively, and lethally in response to any successful large-scale cyberterrorism attack. Participants E1 and P9 argued that the United States would leverage all powers of government following a successful attack, including using the full weight of the military. Further, participant T8 believed that a response would be "lethal for the offending country," participant C4 felt that the United States would respond "forcibly and kinetically," and participant J6 similarly believed the country would respond with "overwhelming forces." Finally, participant B2 stated that the United States will use any means to go after everyone responsible for the successful cyberterrorism attack and would not minimize the response in an attempt to match a cyberattack with a cyber-response.

Theme 4: Cyberterrorism Prevention Measures

All participants agreed that the United States must do a better job aligning different aspects of government to prevent large-scale cyberattacks, to include cyberterrorism attacks. Additionally, most participants agreed that the United States must drastically improve large-scale cyberattack preparations, while some participants highlighted that having a public cyber deterrence policy would help thwart cyberattacks before they begin. The two categories in this theme, *collective coordination* and *preparation*, are the second and third largest categories in this study but make up the most cumulative codes of all themes.

Collective Coordination

Most participants agreed that the United States does not defend as a nation in cyberspace. Participants P3 and J6 stated that the country continues to rely on companies to defend themselves against cyberattacks. For example, participant J6 explained that, “you would never expect Target or Walmart to defend against Russian Bear bombers” since “it’s the job of the U.S. government to buy surface-to-air missiles.” And yet “in cyberspace, not only Target and Walmart, but every little mom-and-pop shop must individually defend for themselves.” Because of this, participant E1 argued that every city, state, and locality must currently take charge of its own cyber defenses.

Participant P3 explained that cyber coordination varies amongst government organizations, though every organization wants a role including the National Security Agency, the Department of Homeland Security, and the Cybersecurity and Infrastructure Agency. Yet, the general lack of coordination amongst all government organizations poses a risk. Participants C4 and J6 agreed that the National Security Agency has the most cybersecurity expertise within the U.S. government, but other government organizations are slowed by “relentless and grinding bureaucracy.” Participant C4 highlighted that his job is focused on weaving U.S. organizations together into a collective cyber defense. Through this, he noted that every private and public organization have their own self-interests and therefore push their own agendas which range from innovative to entrenched and archaic thinking. Participant P9 saw the most cyber innovation in economic and national security organizations, though he believed the expertise drops off drastically within manufacturing and energy based organizations. He also noted that organizations all speak their own languages and do not fully understand each other. Finally, participant T5 believed that coordination between different government agencies is slowly happening but felt there is still a lot that must be done before organizations could be considered integrated.

Participant C4 argued that the United States needs to bridge the public-private divide and shift thinking from the multitude of ad hoc efforts to supporting a national cyber strategy backed by strong leadership. However, participant J6 cautioned that the country might not yet be ready to think in collective cyber defense terms. For example, participant P9 explained that Cyber Command is developing and expanding its own capabilities, clandestine organizations such as the Central Intelligence Agency and elements of Joint Special Operations Command continue to run their own operations in seclusion, and the Federal Bureau of Investigation largely works on their own with the help of National Security Agency operators. Participant J6 highlighted that this channelized mindset often causes overlap in cyberspace which has been a hindrance to the successful coordination of cyber operations. Finally, participant E1 stated that the growth of Cyber Command is a positive step for the Department of Defense, but he explained that there is no comparable organization for the broader U.S. infrastructure since the Department of Homeland Security does not have the authority over civilian federal government systems in the same way that Cyber Command does over the Department of Defense.

Most participants felt that the U.S. government must do more to improve collective cyber measures. Participants B2, J6, and P9 argued that the government should limit compartmentalized information and share cyber intelligence with the private sector in real time. Yet, participant B2 felt that the government is plagued with a culture of secrecy which hinders private sector cooperation. For example, he stated that the government, for the most part, gathers information from the private sector, classifies it, and then does not share any results. He explained that because of this, some of the best cybersecurity experts in the world do not want to deal with the U.S. government since they view the government as an illegitimate partner.

Nevertheless, participant P9 felt that the government must be more directive with at least some parts of the private sector in terms of what cyber security they adapt. He acknowledged that the government has attempted to get the private sector to do more, though only through voluntary initiatives since, as participant C4 explained, the government legally cannot do much to force cyber protection on private companies.

Participants P3 and C4 therefore stated that private companies are largely fighting individually and are on their own. Participant C4 believed that companies with strong resources understand the cyber risk and are generally trying to defend themselves against cyberattacks. For example, he explained that the financial sector recognizes the problem. “They can hire and fire cyber people. They can fund salaries that are super competitive. And they've therefore built some of the best security on the planet.” However, participant

P9 explained that cyber protection tapers off in other government sectors for reasons including limited cyber resources and outdated infrastructure such as old railroad technology.

Preparation

Most participants agreed that the United States can improve large-scale cyberterrorism attack preparations through an overarching strategy and a set policy. Participant P9 felt that the United States should advertise a cyber strategy to ensure that adversaries are aware of potential U.S. responses to any actions, while participant E1 believed that the United States would not be able to respond as effectively to any cyberattack without a set policy. Participants C4 and T8 were generally not satisfied with U.S. preparations for a large-scale terrorism attack, and participant P3 felt that the United States is only prepared well for things that easily transition into mitigating circumstances and is unprepared for cyberterrorism attacks that are not clearly understood and might also take longer to develop. However, he acknowledged that there are venues that exist to bring together federal, state, and military cyber groups to discuss cyberattack preparations.

Participants E1 and B2 felt that U.S. government cyber efforts should focus more on the defensive side, and participant T5 also believed the government should expand cyber measures to improve pre-attack intelligence. Lastly, participant B2 explained that almost everything industrial operates on computers which means that all systems are all vulnerable, including air gapped systems not directly connected to the internet. Because of this, participant T8 felt that improving software would help limit these vulnerabilities while participant P9 argued the United States needs to do a better job hardening potential cyber targets that the country is most dependent on.

Finally, most participants agreed that the United States is not prepared to deter in cyberspace. The reasons include hesitation, unwillingness to expose classified information, attribution uncertainty, a lack of preparation, and general unfamiliarity with cyberspace operations. These participants also felt that the United States cultivates a more dangerous future every time the country does not respond publicly to known cyberattacks.

Participant J6 believed that the United States has allowed too much to go on in the cyber realm without responding. He used the Sony Pictures Entertainment cyberattack by North Korean hackers as an example and explained that the United States would respond if North Korean soldiers physically attacked Sony Pictures and started destroying computers. Yet, there was no public U.S. retaliation for the physical damage caused by the North Koreans using cyber means within the United States. Participant J6 further stated that the United States has never announced how the country would retaliate from a large-scale cyberattack which raises the risk that an adversary might wrongly assume they can get away with something that would subsequently force the United States to act.

Theme 5: Cyberterrorism Policy Agendas

Many experts cannot independently create change and must rely on decision-makers to action their ideas. All participants in this study have national security experience and have therefore all interacted with leaders and lawmakers at some level to facilitate change. Cyberspace is a new and constantly evolving dimension that only the most technical savvy individuals completely understand. Yet, incorporating technical heavy cyberterrorism related information into senior decision-makers' already constrained agendas poses a challenge for cyber and terrorism experts which is highlighted in this theme. Policymaker problems and suggested cyber related improvements are relayed in the theme's three categories: *technical knowledge*, *policymaker consciousness*, and *agenda change factors*. These categories contain approximately one-third of the study's codes reflecting the importance given to cyber policy agendas by the study's participants.

Technical Knowledge

All participants felt that there is not enough cyber understanding on the part of decision-makers. Participant E1 pointed out that may individuals holding high-level government positions have no experience with intelligence issues, so even explaining the differences between the Central Intelligence Agency and the National Security Agency, for example, would be required before progressing to the more technical aspects of cyberspace. Participant C4 similarly felt that cyber policy construction is difficult if policymakers do not understand the technical aspects. Participant A7 took this idea a step further and stated that decision-makers generally have trouble even parsing out the conception of cyberterrorism itself. She felt the challenge is for senior leaders to conceptualize topics consisting of complicated technology with enough nuance and understanding. For example, decision-makers should be able to navigate cyberthreats of completely different types, problems, capabilities, and actors. However, participant P9 believed there is some misunderstanding that cyber policy is more technical than it is in reality. Lastly, participant C4 explained that part of the reason that there are a shortage of decision-makers with technical knowledge is because technologically inclined individuals prefer to stay away from policymaking, so it is also incumbent for these individuals to learn policymaking just as it is for policymakers to become familiar with cyber's technical aspects.

Policymaker Consciousness

This category highlights decision-maker improvements related to cyber policy as witnessed by participants, as well as discussing what generally garners the most attention amongst decision-makers in each participant's respective field. Participant P9 stated that decision-makers are afraid of cyber to some extent. He explained that, "you don't have to be a coder to understand the policy implications of cyber issues just as you don't have to be a nuclear scientist to understand nuclear policy implications." He felt that while people are still hesitant to get involved in cyber topics, involvement has been improving through long term learning and education. Participant P9 also saw a parallel from the private sector in that the appreciation of cybersecurity issues amongst CEOs has also been slowly improving. However, he noted that cyber concerns are very uneven among industries and sectors and felt that there is still a long way to go before cybersecurity is seen as a core issue of national security and diplomacy. Participant E1 felt that cybersecurity will not be seen as a core issue until the topic is raised sufficiently by a U.S. president which he believed has yet to happen.

While there was agreement amongst all participants that decision-makers must devote more attention to cybersecurity issues, there was no agreement on what primarily drives decision-makers. The study’s participants have been exposed to similar areas and similar levels of the U.S. government, yet this category demonstrates that policymakers have varying motivations which makes it difficult to adapt one cyber strategy to trigger policymaker interest.

Participant T5 believed that public opinion mainly drives policymakers, while participants B2 and C4 felt that both the press and individuals in inner circles have the most influence on policymakers. Participant B2 also stated that loss of life, loss of capital, or loss in infrastructure will always get policymakers’ attention, and participant C4 similarity felt that a response to an attack will always take priority. Participant P3 believed policymakers tend to focus on money and perception issues since they do not want to lose money or be perceived badly. Similarly, participant P9 also felt that perception and focusing on any major threats mostly consume policymakers. Participants B3 and J6 stated that immediacy, or the biggest threat of the day, always captures policymakers’ attentions, while participant A7 argued that problems are the main drivers for policymakers. Lastly, participant T5 believed that information received through intelligence often has the potential to become the primary focus of policymakers.

Agenda Change Factors

In this category, participants discussed what would cause cyber policy, to include cyberterrorism policy, to align with mainstream U.S. government agendas. Participant C4 felt that the government contains many well-intentioned and smart people concerned with the country’s cybersecurity, yet something severe would need to happen through cyberspace in order to get leadership focused on the issue. Participants B2 and A7 stated that big negative events would need to occur to capture the attention of decision-makers, though participant B2 was hopeful that cyber professionals are continuing to work hard behind the scenes to move agendas as much as they can in absence of upper-level decision-maker support.

Participant J6 worried that moving the cyber agenda will take a mass causality event or another major crippling event. He explained his logic using the NotPetya attack released by the Russians that caused over 10 billion USD worth of damage worldwide, including hundreds of millions of dollars in the United States, yet caused no large public reactions within the U.S. government. Lastly, participant P9 believed that continued and effective cyberattacks against the United States would at least get policymakers to rethink the country's current stance on cyber activities, while participant T5 hoped that policymakers are growing more concerned with how cyber actions are aiding countries in their worldwide goals that are not in line with U.S. policy, such as the Russian annexation of Crimea.

Theme 6: International Cyberterrorism Considerations

No international law directly addresses cyberterrorism, and it is also not clear how the Geneva Conventions and the greater laws of armed conflict apply to cyberterrorism (Baram & Menashri, 2019; Fidler, 2016; Marsili, 2019). There are additionally no U.S. or international laws directly related to self-defense in cyberspace (Cook, 2018). Given these considerations, the first category in this theme, *international law validity*, addresses to what level the United States should consider international law when drafting cyber plans, to include cyberterrorism plans; while the second category, *international law integration*, gauges the likelihood for agreed upon worldwide cyber regulations.

International Law Validity

Most participants agreed that the United States must acknowledge international law when drafting cyber related deterrence and response plans regardless of how difficult or inconvenient the task. Participant P9 stated that the United States should articulate how international law applies in cyberspace just like in every other area. He further stated that the United States should strive to be champions of the rule of law in all aspects and noted that violating international law in cyberspace would hurt the country's international status. Participant P9 also felt that advertising strong cyber deterrence and response initiatives that follow international law would encourage other countries to do the same and would also serve as a point of emphasis for countries that choose not to follow international law in cyberspace. He lastly pointed out that there are over 40 countries developing offensive cyber capabilities which is why global cyber discussions on cyber norms related to international law are so important, though he did not feel that international law needs to be rewritten for cyberspace.

Participant T5 stated that cyber is global in the sense that any malware released, for example, will spread worldwide regardless of its targeted audience. Given that, he felt that the United States needs to consider international law because any cyber response against one country could have unintended consequences in other countries. Participant P3 highlighted this sentiment by explaining how Russia ceased cyberattacks against Georgia in 2008 after Georgia moved their backup servers to a cloud-based website in the

United States that Russia was not willing to attack. Given that, he felt that international law applies when searching through the networks of other countries to identify weaknesses for future attacks or to even stop an ongoing large-scale cyberattack.

Participant J6 explained that cyber is another domain of warfare, and there are standard rules of warfare that the United States has agreed to that also generally translate to the cyber realm. He therefore felt that cyber is not a fundamentally different domain where the entire rules of warfare need to be rewritten. Participant C4 suggested that the country should even consider international law throughout all cyber related preplans, missions, and activities, while participant E1 acknowledged that cyber is still a developing area but the United States must at least pay attention to and understand how international law relates. Finally, participant B2 argued that international law related to cyberspace is not that helpful but felt that the United States must still consider it in order to demonstrate a willingness to cooperate.

International Law Integration

While most participants agreed that international law applies in cyberspace, they were not optimistic that cyberspace rules or norms will ever be agreed upon in the current international environment. Participant A7 felt that there will never be a cyber treaty between the major world powers given the fundamental disconnects in worldviews. Participant J6 also did not believe there will be a major international-level agreement on cyber issues due to the fundamental divisions between the Western view of the cyber domain and the Russian and Chinese views. For example, participants P3 and J6 stated that China wants cyber treaties that allow them to have power and leverage over their own people and anyone else that they have influence over, and likewise with Russia who sees cyber agreements as a way of ensuring people stay out of their way.

Participant P9 explained that these differences drive huge divisions in intergovernmental forms such as in the UN where major disagreements are seen between Russia and China and Western democracies coupled with Japan, Australia, and others. Participant T8 acknowledged the international cyber divide but pointed out that the United States has also voted down proposals regarding cyber laws and legislation in the UN which participant E1 felt puts the country in an awkward position when it comes to aspects of international law and cyber.

Lastly, participant P9 suggested taking cyber "out of this kind of boutique bubble it is in" and looking at the overall relationship with other countries. To back up this argument, he articulated that one of the reasons China agreed to an intellectual property agreement with the United States in 2015 was because President Obama did not categorize the issue as a cyber issue but instead categorized it as a core economic and national security issue. President Obama was thus willing to have friction over U.S.-China relations as a whole in order to resolve a cyber matter.

Summary

The purpose of this qualitative study was to explore the perceptions of U.S. terrorism and cybersecurity experts with demonstrated federal government experience to understand how the country might better prevent and respond to a successful large-scale cyberterrorism attack. Data were generated through one-on-one semistructured telephone interviews and were coded and categorized into themes in order to draw conclusions. The findings successfully answered the study’s research question: How do terrorism and cybersecurity experts perceive that the United States might better prevent, cope with, and respond to large-scale cyberterrorism attacks?

An answer would be incomplete without first conceptualizing the abilities of terrorists to carry out large-scale cyberterrorism attacks which was articulated in Theme 1. Here, most participants agreed that terrorist cyber capabilities were weak, and the probability of a large-scale cyberterrorism attack was therefore low which was expressed in Theme 2. Theme 3 presented a consensus that the United States would respond quickly, aggressively, and lethally in the event terrorists were able to carry out a successful large-scale terrorism attack. Yet, participants unanimously agreed in Theme 4 that the United States could do much more to prevent destructive cyberattacks, including cyberterrorism attacks, against the country which focused on working together as a nation to form a collective cyber defense front.

However, any U.S. cyberterrorism prevention and response guidelines would require policymaker backing and coordination which was the focus of this study’s theory. Punctuated equilibrium theory was designed to be broadly applied to a range of policymaking initiatives during protracted periods of stability coupled with bouts of immediate change. The theory was thus relevant to this study given that U.S. policymakers are responsible for selecting improved cyberterrorism defense and response policies.

Participants highlighted the lack of technical knowledge amongst policymakers and discussed ways to overcome policymaker cyber shortcomings in Theme 5, though most participants worried that cyber considerations would only be thrust into mainstream national policy discourse following a successful large-scale cyberterrorism attack. The internet, cyber, and most terrorist elements are global by definition, so Theme 6 categorized to what level the United States should consider international law when preparing for or responding to a large-scale cyberterrorism attack. Most participants agreed that international law must be considered regardless of how difficult or inconvenient the task even though an internationally agreed upon cyber treaty is unlikely. Chapter 5 presents the interpretations of the findings. It also discusses the study's limitations, recommendations, and implications and lastly outlines conclusions for this study.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

In this chapter, I provide a summation of the purpose and review the key findings of the study. I then discuss the limitations, recommendations, and implications of the study and finally end with the conclusion. The purpose of this qualitative study was to explore the perceptions of terrorism and cybersecurity experts in the United States to understand how the country might prevent and respond to a large-scale cyberterrorism attack. Through expert interviews, I addressed if additional measures were needed to better handle aspects of any major cyberterrorism attack. This study filled a gap in literature identified through an exhaustive literature review by presenting expert analysis on current U.S. government cyberterrorism policy including the validity of creating U.S. cyberterrorism specific deterrence and response guidelines.

I collected data from nine participants from August 27 to October 3, 2020 using semistructured telephone interviews. All interview questions were aligned with the research question by considering the study's problem, purpose, structure, and theoretical foundation. The six themes that emerged from data analysis were as follows:

- Terrorists' cyber capabilities
- Large-scale cyberterrorism attack probability
- Large-scale cyberterrorism attack likely responses
- Cyberterrorism prevention measures
- Cyberterrorism policy agendas
- International cyberterrorism considerations

Interpretation of the Findings

Through the findings, I successfully answered the study's research question: How do terrorism and cybersecurity experts perceive that the United States might better prevent, cope with, and respond to large-scale cyberterrorism attacks? Most participants agreed that terrorist organizations do not have the organic capability to carry out a large-scale cyberterrorism attack against the United States, so the probability of a successful large-scale cyberterrorism attack against the country is therefore low. However, most participants also agreed that non-state actors could conduct a successful major cyberattack against the United States with state assistance.

The literature review indicated that given these circumstances, the onus would be on the United States to correctly attribute the cyberattack and levy retribution accordingly. Most participants were satisfied with the United States' ability to attribute cyberattacks with a high degree of confidence. Participants also unanimously agreed that the United States would respond quickly, aggressively, and lethally in response to a successful large-scale cyberattack and would not restrict responses to the cyber realm.

Information in the literature review emphasized that the United States would likely consider a state assisted cyberterrorism attack an act of war by the belligerent government and would respond in accordance with international law. I therefore concluded that the United States does not need to consider specific large-scale cyberterrorism attack response options since terrorists likely do not possess the capabilities to carry out an attack, and the United States would consider a state assisted large-scale cyberterrorism attack an act of war from the offending country.

However, participants also unanimously agreed that the United States could do much more to prevent destructive cyberattacks, including cyberterrorism attacks, through deterrence. Yet, any progress in U.S. cyberterrorism deterrence would require policymaker backing and coordination in both pre- and potentially post-attack environments. Experts must therefore observe and navigate U.S. government institutional friction described in these environments by punctuated equilibrium theory in order to offer improvements for cyberterrorism deterrence guidelines.

I used punctuated equilibrium theory to conceptualize expert cyberterrorism deterrence improvements in two very different environments in this study. Most participants highlighted the lack of technical knowledge amongst U.S. policymakers and agreed that cyber considerations would only be integrated into mainstream national policy discourse following a successful large-scale cyberterrorism attack against the country. In accordance with punctuated equilibrium theory, policymakers have demonstrated large-scale cyberattack complacency through bounded rationality and will likely overreact in the chaotic environment following a catastrophic cyberattack which could be problematic. However, most participants agreed that the United States would still be cognizant of international law when responding to a highly destructive cyberattack absent of any pre-drafted plans. I finally concluded that the United States must significantly improve cyberterrorism attack deterrence guidelines, but the country is not in danger of violating international law in the absence of this guidance.

Limitations of the Study

The main limitation of this study was the potential for incomplete information due to a limited number of participants. I identified a small pool of 89 potential participants meeting expert criteria for this study and drew data from only nine of those participants covering a topic that is relevant for scores of private and public organizations throughout the United States. Furthermore, all study participants worked in various government, security, legislation, and educational sectors so the perceptions of their knowledge could have been skewed by their own lived experiences. Another major limitation of this study was not knowing what controlled or classified information and guidance exists within the many U.S. government layers for preventing and responding to cyberattacks. Lastly, it was imperative for me to attempt to mitigate all potential biases as a new researcher to not inadvertently damage the integrity of the study.

Recommendations

The opportunities for further research are broad. In this study, I highlighted many areas for improvement including a lack of technical cyber education amongst U.S. policymakers, a lack of cyberterrorism defense coordination between and amongst U.S. public and private organizations, the reluctance of the U.S. government to distribute cyber related intelligence, and the absence of cyberterrorism issues amongst top national policy agendas. Each of these areas could be researched individually or as part of a broader theme to further investigate the absence of cyberterrorism within the U.S. national defense architecture. One major limitation for the study was not knowing what classified information exists relating to U.S. cyberterrorism defense initiatives. Therefore, a classified level cyberterrorism study could offer relevant policymakers a more complete view of the topic. Additionally, further research could be conducted with U.S. government support to include a broader sample of experts using both qualitative and quantitative methods in order to gain a deeper and more exact understanding of cyberterrorism focused issues. Lastly, this study could be rerun using similar methods in the future to gauge the developments of U.S. national policy and policymaker attitudes toward aspects of cyberterrorism.

Implications

The theoretical framework for this study was intended to be broadly applied to a range of policymaking initiatives focusing on policy change driven by political organizations during protracted periods of stability coupled with bouts of immediate change. The findings of this study addressed the high relevance of punctuated equilibrium theory since U.S. policymakers are the gatekeepers to improved cyberterrorism related policies. Specifically, I highlighted the need for better collective defense and prevention measures against large-scale cyberattacks in Theme 4. Yet, I demonstrated the reluctance of policymakers to address these issues in the absence of a successful large-scale cyberattack in Theme 5.

Therefore, punctuated equilibrium theory implications suggest that it would be incumbent on cyber experts to drive awareness from within and amongst organizations while simultaneously championing cyberterrorism policy consciousness since policymakers are likely not intrinsically motivated to focus on the issue. Moreover, the overarching implications of punctuated equilibrium theory can be applied to research focusing on all national policy agendas.

The implications for social change are vast. At a minimum, this study can contribute to dialogue on a number of issues absent in cyberterrorism literature discourse discussed in the results, including tracking terrorists' cyber capabilities and improving the collective national cyber defense for small private businesses to large government organizations. Many advancements are required to create a unified U.S. cyber defense front along with associated policies. Future research could therefore explore improved cyberattack preparedness holistically or broken down into its many shortcomings presented in Theme 4.

Theme 5 also addressed the lack of cyberterrorism knowledge amongst U.S. policymakers, so this study can also be used to encourage greater policymaker cyberterrorism awareness through education and through requiring the synthesis of cyber related information from government organizations in order to make accurate determinations. Lastly, a recommendation generated from the results of this study would be to closely monitor terrorist organizations' digital developments since continuous innovation in cyberspace could eventually lead to a *cyber 9/11* breakthrough, and the United States will need to be ready with deterrence and response options when that happens.

Conclusion

In this research study, I sought to determine if the United States needed cyberterrorism-specific deterrence and response guidelines in order to better prepare for and respond to successful large-scale cyberterrorism attacks. A thorough literature review found that the United States has not established cyberterrorism guidelines, with information generally being nonexistent on the topic, and I wanted to figure out why. I interviewed nine highly qualified cyber and terrorism experts to gather information and discovered different reasons for why the United States does not have cyberterrorism deterrence guidelines and why the country also does not have similarly specific response guidelines.

The United States presents a very weak cyber defense posture, which most participants in this study felt needed improvement, due primarily to policymaker inattention but also as a result of highly individualistic cyber defense efforts amongst virtually all U.S. organizations. Furthermore, the United States does not have cyberterrorism specific response guidelines primarily because terrorist organizations most likely do not have the capability to organically conduct a successful large-scale cyberterrorism attack.

However, cyber technologies are exponentially increasing in sophistication and proliferation which does not necessarily align with the metered and reflective progress of the U.S. government and could thus be problematic. Every U.S. policymaker will be well versed on cyberterrorism following a successful large-scale cyberterrorism attack, but likely not until then. It is therefore incumbent on cyber experts nationwide to surreptitiously improve defenses, raise awareness, and drive change until cyberspace is intuitively comprehended by a technically astute generation at some point in the future, and hopefully not as the result of a destructive cyberterrorism attack within the United States.

References

Albahar, M. (2019). Cyber attacks and terrorism: A twenty-first century conundrum. *Science and Engineering Ethics*, *25*, 993–1006. https://www.doi.org/10.1007/s11948-016-9864-0

Baram, G., & Menashri, H. (2019). Why can't we be friends? Challenges to international cyberwarfare cooperation efforts and the way ahead. *Comparative Strategy*, *38*(2), 89–97. https://doi.org/10.1080/01495933.2019.1573069

Barrett, E. (2017). On the relationship between the ethics and the law of war: Cyber operations and sublethal harm. *Ethica & International Affairs*, *31*(4), 467–477. https://doi.org/10.1017/S0892679417000454

Baumgartner, F. M., Jones, B. D., & Mortensen, P. B. (2018). Punctuated equilibrium theory: Explaining stability and change in public policymaking. In C. M. Weible, & P. A. Sabatier (Eds.), *Theories of the policy process* (4th ed., pp. 71–132). Routledge. https://lccn.loc.gov/2017009463

Boeke, S., & Broeders, D. (2018). The deminitarisation of cyber conflict. *Survival*, *60*(6), 73–90. https://doi.org/10.1080/00396338.2018.1542804

Boo, H. W. (2017). An assessment of North Korean cyber threats. *The Journal of Eastern Asian Affairs*, *31*(1), 97–117. https://www.jstor.org/stable/44321274

Boys, J. D. (2018). The Clinton administration's development and implementation of cybersecurity strategy (1993–2001). *Intelligence and National Security*, *33*(5). https://doi.org/10.1080/02684527.2018.1449369

Bracken, P. (2017). Cyberwar and its strategic context. *Georgetown Journal of International Affairs*, *18*(3), 147–157. https://doi.org/10.1353/gia.2017.0047

Bracknell, B. (2016). NATO approaches in response to ISIL and international terrorism. *International Lawyer*, *49*(3), 417–426. https://scholar.smu.edu/cgi/viewcontent.cgi?article=4470&context=til

Brantly, A. F. (2016). The most governed ungovened space: Legal and oplicy constraints on military operations in cyberspace. *SAIS Review*, *36*(2), 29–39. https://doi.org/10.1353/sais.2016.0018

Bureau of Counterterrorism. (n.d.). *Foreign terrorist organizations*. U.S. Department of State. Retrieved May 19, 2020, from https://www.state.gov/foreign-terrorist-organizations/

Caplan, N. (2013). Cyber war. The challenge to national security. *Global Security Studies 4*(1), 93–115. http://globalsecuritystudies.com/Caplan%20Cyber.pdf

Congressional Research Service. (2019). *U.S.-China tariff actions by the numbers.* https://fas.org/sgp/crs/row/R45949.pdf

Cook, C. (2018). Cross-Border data access and active cyber defense: Assessing legislative options for a new international cybersecurity rulebook. *Stanford Law & Policy Review*, *29*(2), 205–236. https://law.stanford.edu/wp-content/uploads/2018/08/SLPR_Cook.pdf

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Sage.

Dev, P. R. (2015). "Use of force" and "armed attack" thresholds in cyber conflict: The looming definitional gaps and the growing need for formal U.N. response. *Texas International Law Jounral*, *50*(2), 379–399. https://texashistory.unt.edu/ark:/67531/metapth838918/

Dinniss, H. A. (2018). The threat of cyber terrorism and what international law should (try to) do about it. *Georgetown Journal of International Affairs*, *19*, 43–50. https://doi.org/10.1353/gia.2018.0006

Dorn, W. (2018). Cyberpeacekeeping: A new role for the United Nations? *Georgetown Journal of International Affairs*, *18*(3), 138–146. https://muse-jhu-edu.ezp.waldenulibrary.org/article/700309

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice. *American Journal of International Law*, *112*(4), 583–657. https://doi.org/10.1017/ajil.2018.86

Fatalities. (n.d.). United Nations peacekeeping. Retrieved November 27, 2020 from, https://peacekeeping.un.org/en/fatalities

Federica, G. (2018). NATO's enhanced role in counter terrorism. *Defence Against Terrorism Review*, *10*, 9–20. https://www.tmmm.tsk.tr/publication/datr/volume_10/01_NATOs_Enhanced_Role_in_CounterTerrorism.pdf

Fenton, H. A. (2019). Proportionality and its applicability in the realm of cyber-attacks. *Duke Journal of Comparative & International Law*, *29*(2), 335–339. https://scholarship.law.duke.edu/djcil/vol29/iss2/6

Fidler, D. P. (2016). Cyberspace, terrorism and international law. *Journal of Conflict & Security Law*, *21*(3), 475–493. https://doi.org/10.1093/jcsl/krw013

Finlay, L., & Payne, C. (2019). The attribution problem and cyber armed attacks. *American Journal of International Law*, *113*, 202–206. https://doi.org/10.1017/aju.2019.35

Flink, C. M. (2017). Rethinking punctuated equilibrium theory: A public administration approach to budgetary changes. *The Policy Studies Journal*, *45*(1), 101–120. https://doi.org/10.1111/psj.12114

Gaibulloev, K., & Sandler, T. (2019). Terrorism and affinity of nations. *Public Choice, 178*, 329–347. https://doi.org/10.1007/s11127-018-0611-8

Ghatak, S., Gold, A., & Prins, B. C. (2019). Domestic terrorism in democratic states: Understanding and addressing minority grievances. *Journal of Conflict Resolution*, *63*(2), 439–467. https://doi.org/10.1177/0022002717734285

Goode, A. C. (2015). Cyberterrorists: The identification and classification of non-state actors who engage in cyber-hostilities. *Military Law Review*, *223*(1), 157–197.

H.R.3270 - Active Cyber Defense Certainty Act. (n.d.). Congress.gov. Retrieved May 18, 2020, from https://www.congress.gov/bill/116th-congress/house-bill/3270

Haber, E., & Zarsky, T. (2017). Cybersecurity for infrastrucutre: A critical analysis. *Florida State University Law Review*, *44*(2), 515–578. https://ir.law.fsu.edu/lr/vol44/iss2/3

Hansen, H. E., Memeth, S. C., & Mauslein, J. A. (2020). United Nations peacekeeping and terrorism: Short-Term risks and long-term benefits. *International Interactions*, *46*(2), 199–226. https://doi.org/10.1080/03050629.2020.1725500

Hatch, B. B. (2018). Defining a class of cyber weapons as WMD: An examination of the merits. *Journal of Strategic Study*, *11*(1), 43–61. https://doi.org/10.5038/1944-0472.11.1.1657

Healey, J. (2018). Who's in control: Balance in cyber's public-private sector partnerships. *Georgetown Journal of International Affairs*, *18*(3), 120–130. https://doi.org/10.1353/gia.2017.0044

Hellmuth, D. (2018a). More similar than different: Of checks, balances, and German and American government responses to international terrorism. *German Politics*, *27*(2), 265–281. https://doi.org/10.1080/09644008.2018.1443774

Hellmuth, D. (2018b). Of terrorism types and countermeasures: In need of a new framework. *Comparative Strategy*, *37*(3), 155–174. https://doi.org/10.1080/01495933.2018.1486081

Hodgkinson, S. L. (2018). Crossing the line: The law of war and cyber engagement - applying the existing boby of law to this new national security threat. *International Lawyer*, *51*(3), 613–628.

Hoffman, B. (2017). *Inside terrorism* (3rd ed.). Columbia University Press.

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime and Delinquency*, 778–872. https://doi.org/10.1177/0011128712452963

Hughes, M. J. (2011). British opinion and Russian terrorism in the 1880s. *European History Quarterly, 41*(2), 255–277. https://doi.org/10.1177/0265691411399039

Jarvis, L., & Macdonald, S. (2015). What is cyberterrorism? Findings from a survey of researchers. *Terrorism and Political Violence*, *27*(4), 657–676. https://doi.org/10.1080/09546553.2013.847827

Jasko, K., LaFree, G., & Kruglanski, A. (2017). Quest for significance and violent extremism: The case of domestic radicalization. *Political Psychology*, *38*(5), 815–831. https://doi.org/10.1111/pops.12376

Jenkins, B. M., & Godges, J. P. (2011). *The long shadow of 9/11: America's response to terrorism.* RAND corporation. https://www.rand.org/pubs/monographs/MG1107.html

Karlsrud, J. (2017). Towards UN counter-terrorism operations? *Third World Quarterly, 38*(6), 1215–1231. http://dx.doi.org/10.1080/01436597.2016.1268907

Klein, J. J. (2015). Deterring and dissuading cyberterrorism. *Journal of Strategic Study*, *8*(4), 23–38. http://dx.doi.org/10.5038/1944-0472.8.4.1460

Koski, C., & Workman, S. (2018). Drawing practical lessons from punctuated equilibrium theory. *Policy & Politics*, *46*(2), 293–308. https://doi.org/10.1332/030557318X15230061413778

Kosseff, J. (2018). Defining cybersecurity law. *Iowa Law Review*, *103*(3), 985–1031. https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/

Kuhlmann, J., & Van der Heijden, J. (2018). What is known about punctuated equilibrium theory? And what does that tell us about the construction, validation, and replication of knowledge in the policy sciences? *Review of Policy Research*, *35*(2), 326–347. https://doi.org/10.1111/ropr.12283

László, K. (2018). Cyber security policy and strategy in the European Union and NATO. *Revista Academiei Forţelor Terestre*, *23*(1), 16–24. https://doaj.org/article/229c48348c894f07a5c5d59280edb5a5

Loleski, S. (2019). From cold to cyber warriors: The origins and expansion of NSA's tailored access operations (TAO) to shadow brokers. *Intelligence and National Security*, *34*(1), 112–128. https://doi.org/10.1080/02684527.2018.1532627

Marsili, M. (2019). The war on cyberterrorism. *Democracy and Security*, *15*(2), 172–199. https://doi.org/10.1080/17419166.2018.1496826

Matwyshyn, A. M. (2018). CYBER!. *Brigham Young University Law Review*, *2017*(5), 1109–1196. https://digitalcommons.law.byu.edu/lawreview/vol2017/iss5/6/

Mazanec, B. M. (2016). Constraining norms for cyber warfare are unlikely. *Georgetown Journal of International Affairs*, *17*(3), 100–109. https://doi.org/10.1353/gia.2016.0040

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation.* Wiley.

Mori, S. (2019). US technological competition with China: The military, industrial and digital network dimensions. *Asia-Pacific Review*, *26*(1), 77–120. https://doi.org/10.1080/13439006.2019.1622871

Morkevičius, V. (2015). Power and order: The shared logics of realism and just war theory. *International Studies Quarterly*, 11–22. https://doi.org/10.1111/isqu.12152

Morse, J. M. (1994). *Designing funded qualitative research.* Sage.

Naím, M. (2017). Why democracies are at a disadvantage in cyber wars. *Journal of International Affairs*, *70*, 1–4. https://jia.sipa.columbia.edu/democracies-disadvantage-cyber-wars

Nance, M., & Sampson, C. (2017). *Hacking ISIS. How to destroy cyber jihad.* Skyhorse Publishing.

National Commission of Terrorist Attacks upon the United States. (2004). *The 9/11 commission report: Final report on the national commission on terrorist attacks upon the United States* (1st ed.). https://9-11commission.gov/report/

Neely, P. R., & Allen, M. T. (2018). Policing cyber terrorism. *Journal of Cybersecurity*, *3*(1), 13–18. https://doi.org/10.19030/jcr.v3i1.10227

Noone, H. (2019). Two-Level games and the policy process: Assessing domestic-foreign policy linkage theory. *World Affairs*, *182*(2), 165–186. https://doi.org/10.1177/0043820019839074

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Office of Public Affairs. (2016). *ISIL-Linked Kosovo hacker sentenced to 20 years in prison*. Department of Justice. https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison

Osawa, J. (2017). The escalation of state sponsored cyberattack and national cyber security affairs: Is strategic cyber deterrence the key to solving the problem? *Asia-Pacific Review*, *24*(2), 113–131. https://doi.org/10.1080/13439006.2017.1406703

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Sage.

Podgor, E. S. (2002). Computer crimes and the USA PATRIOT act. *Criminal Justice*, *17*(2). https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=196247

Qureshi, W. A. (2019). Fourth- and fifth-generation warfare: Technology and perceptions. *San Diego International Law Journal*, 187–216. https://digital.sandiego.edu/ilj/vol21/iss1/7

Rapoport, D. C. (2013). The four waves of modern terror: International dimensions and consequences. In J. M. Hanhimaki, & B. Blumenau (Eds.), *An international history of terrorism* (pp. 282–310). Routledge. https://doi.org/10.4324/9780203093467

Rapoport, D. C. (2016). It is waves, not strains. *Terrorism and Political Violence*, *28*(2), 217–224. https://doi.org/10.1080/09546553.2015.1112278

Rich, P. B. (2013). Understanding terror, terrorism, and their representations in media and culture. *Studies in Conflist & Terrorism*, *36*(3), 255–277. https://doi.org/10.1080/1057610X.2013.755915

Roberts, A. (2015). Terrorism research: Past, present, and future. *Studies in Conflict & Terrorism*, *38*(1), 62–74. https://www.doi.org/10.1080/1057610X.2014.976011

Rudestam, K. E., & Newton, R. R. (2015). *Surviving your dissertation: A comprehensive guide to content and process* (4th ed.). Sage.

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Sage.

Schulzke, M. (2018). The politics of attributing blame for cyberattacks and the costs of uncertainty. *Perspectives on Politics*, *16*(4), 954–968. https://doi.org/10.1017/S153759271800110X

Shad, M. R. (2018). Cyber threat in interstate relations: Case of US-Russia cyber tensions. *Policy Perspectives*, *14*(2), 41–55. https://doi.org/10.13169/polipers.15.2.0041

Shor, E. (2016). Counterterrorist legislation and subsequent terrorism: Does it work? *Social Forces*, *95*(2), 525–557. https://doi.org/10.1093/sf/sow052

Sleat, M. (2017). Just cyber war?: Casus belli, information ethics, and the human perspective. *Review of International Studies*, *44*(2), 324–342. https://doi.org/10.1017/S026021051700047X

Tabansky, L. (2018). Sticking to their guns: The missing RMA for cybersecurity. *Military Cyber Affairs*, *3*(1), 1–21. https://doi.org/10.5038/2378-0789.3.1.1039

Taylor, I. (2017). Just war theory and the military response to terrorism. *Social Theory & Practice*, 717–740. https://www.jstor.org/stable/26405304

Tehrani, P. M. (2017). *Cyberterrorism: The legal and enforcement issues*. World Scientific Publishing Europe Ltd.

UN. (1945, June 26). *Charter of the United Nations.* United Nations. https://www.un.org/en/charter-united-nations/index.html

Van Dine, A. (2020). When is cyber defense a crime? Evaluating active cyber defense measures under the Budapest Convention. *Chicago Journal of International Law*, *20*(2), 532–563. https://chicagounbound.uchicago.edu/cjil/vol20/iss2/18

Walzer, M. (2007). *Michael Walzer on terrorism and just war*. IAS. https://www.ias.edu/ideas/2007/walzer-terrorism-just-war

Warf, B., & Fekete, E. (2016). Relational geographies of cyberterrorism and cyberwar. *Space and Polity*, *20*(2), 143–157. https://doi.org/10.1080/13562576.2015.1112113

Weiss, M., & Jankauskas, V. (2018). Securing cyberspace: How states design governance arrangements. *Governance*, *32*(2), 259–275. https://doi.org/10.1111/gove.12368

White, J. (2016). Cyber threats and cyber security: National security issues, policy and strategies. *Global Security Studies*, *7*(4), 24–33. http://www.globalsecuritystudies.com/White%20Cyber.docx.pdf

Wilner, A. S. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*, *43*(2), 245–280. https://doi.org/10.1080/01402390.2018.1563779

Wirtz, J. J. (2017). The cyber Pearl Harbor. *Intelligence and National Security*, *32*(6), 758–767. https://doi.org/10.1080/02684527.2017.1294379

Appendix A: Interview Protocol

Introduction

Before I begin the recording, I just wanted to reconfirm that you agree to the consent form, are still willing to participate, and have no final questions.

[Audio recording starts here after consent form is confirmed]

Opening

Thank you for taking time to participate in this research study on *Deterrence and Response Improvements for a Large-Scale Cyberterrorism Attack.* As you know, I am Harrison Cunningham, a Ph.D. student at Walden University. The purpose of this study is to explore the perceptions of terrorism and cybersecurity experts in the United States to understand how the country might better prevent and respond to a large-scale cyberterrorism attack. The findings of this study may help U.S. government policymakers determine if large-scale cyberterrorism attack guidelines could be improved in order to better prevent and respond to any major attack. This conversation is confidential, and your identity will be protected using a code created specifically for this study.

Interview Questions

The next 18 questions are open-ended. I will ask one question at a time and then give you as much time as you need to respond. Please be as detailed as possible with your responses. If you are unable to answer a question, just let me know and we will move on to the next one. There may be times when I will ask probing questions to get deeper responses or for clarification, but I will not ask questions with the intent of attempting to draw you to a particular answer. Let's begin.

[Begin the interview research questions in Appendix B]

Conclusion

That concludes the questions. Thank you again for your time. The next step for me will be to transcribe this interview and send you a copy that you can edit as you desire. Please send any edits back to me as soon as you can after you receive the transcription. If you have any questions, please feel free to contact me.

Appendix B: Interview Questions

Opening Questions

1. What is your profession?
2. What is your role in your current profession?
3. How many years have you worked in your current profession?
4. How many years have your professional responsibilities been associated with aspects of cyber or terrorism?
5. What have been the different focuses in your current area of expertise?

Research Question Focused Questions

6. What have been the biggest priorities of executives and decision-makers senior to you?
7. What do you view as the greatest risks to U.S. national security?
8. Please explain your understanding of cyberterrorism.
9. How much common understanding regarding aspects of cyber and terrorism do you see across organizations that have the ability to influence national cyberterrorism policy?
10. How likely do you think it is that terrorists currently possess capabilities to conduct a large-scale cyberattack against the United States? Please explain.
11. Describe your overall satisfaction with U.S. preparations for large-scale cyberterrorism attacks.
12. In your opinion, what precautionary measures, if any, can the United States implement to minimize the threat of a large-scale cyberterrorism attack?
13. To what extent should the United States consider international law when preparing for or responding to a large-scale cyberterrorism attack?
14. How do you think the United States would respond to a successful large-scale cyberterrorism attack with results comparable to or greater than 9/11?

Punctuated Equilibrium Focused Questions

15. What do you think influences the perceptions of national policy makers related to your area of expertise?
16. What are the main drivers of the most important policy issues relating to your area of expertise?
17. What positive or negative external factors have affected aligning cyberterrorism awareness with the national security agenda? Please explain.

Closing Question

18. What additional information can you provide related to attacks against the United States utilizing cyber or terrorism means?

Appendix C: Second Cycle Codes

Code Name	Participants	1st Cycle Codes	Interview Questions (times referenced)
Theme 1: Terrorists’ Cyber Capabilities			
cyber competence	J6, A7	3	6, 8, 10
limited cyber sophistication	C4, J6, P9	3	8, 10(2)
hire cyber capability	B2, P9	3	9(2), 10
cyberattacks not limited to nations	B2	3	5, 8(2)
cyberattacks primarily state	E1, P3	2	8, 10
“serve as proxies”	C4	1	10
Theme 2: Large-Scale Cyberterrorism Attack Probability *Category 1*: *Low Probability*			
low probability	C4, J6, A7, T8, P9	6	10(5), 14
has been overblown	E1	2	8, 10
attack is likely	B2	2	5(2)
“skeptic about the threat”	E1	1	11
Category 2: *Activity Below War Threshold*			
probing	E3, T5, A7	3	10(2), 11
weaponizing espionage	T5, T8, P9	3	7, 10, 11
“reluctant to respond”	P9, E1	2	12, 14
espionage	B2, C4	2	8, 10
terrorism disinterest	P9, J6	2	6, 8
“operating below brink of warfare”	C4	1	10
Theme 3: Large-Scale Cyberterrorism Attack Likely Responses *Category 1*: *Attribution Considerations*			
attribution considerations	C4, J6	2	8, 14
attribution capabilities	E1, P9	2	6, 10
attribution improvements	B2, P9	2	14(2)
“private providers don’t worry about attribution”	P3	1	11
“attribution would be swift”	T8	1	14
“easy to disguise stuff”	B2	1	14

Code Name	Participants	1st Cycle Codes	Interview Questions (times referenced)
Category 2: *Lethal Response*			
large lethal response	E1, B2, C4, J6, T8, P9	7	10(2), 13, 14(3), 16
good physical disaster response	P3	1	14
Theme 4: Cyberterrorism Prevention Measures *Category 1*: *Collective Coordination*			
strive for collective defense	P3, C4, T5, J6	6	6, 7, 9(2), 11, 14
better government info sharing	B2, J6, P9	6	8, 11(3), 12(2)
bad agency coordination	C4, P9	4	9(2), 11, 16
get private sector to do more	C4, P9	4	6, 9, 11, 12
individual industry preparedness	E1, P3, P9	3	9, 12, 14
US cyber command developments	E1, J6, P9	3	10, 11(2)
industry leading technology	E1, T5, J6	3	6, 12(2)
private sectors are on their own	P3, C4	3	8, 9, 11
need better government coordination	C4, J6	3	6, 9, 12
private sector divisions	C4, P9	3	9(2), 17
work with allies	T8, P9	3	12(2), 13
more government involvement	J6, P9	2	6, 12
splintered cyber defense	J6, A7	2	11, 12
“private sector was actually willing”	B2	1	7
“military taking on a more prominent role”	P9	1	9
“give them actual tools they can use”	J6	1	12
“moderating content online”	A7	1	16
Category 2: *Preparation*			
set strategy and policy	E1, P3, C4, T8, P9	6	10(2), 11(3), 14
hardware and software advances	B2, P3, T8, P9	6	6, 11, 12(2), 14, 17
no public deterrence	B2, J6, P9	4	7, 8, 12, 13
network vulnerabilities	B2, P3, T5	3	8, 10, 14
threat disruptions	C4, J6	3	8, 11, 12
step up actions	T5, P9	2	7, 12
defensive improvements	E1, T5	2	12(2)
intelligence system solutions	T5, A7	2	12(2)
overall strategic plan	A7, P9	2	12(2)

Code Name	Participants	First Cycle	Interview Questions (times referenced)
“government structures are still administratively driven”	P3	1	7
“we’ve really started pushing back”	J6	1	8
“be prepared for it”	P3	1	10
“streamline the legal authorities”	C4	1	13
“we’ve allowed too much to go on”	J6	1	16
“assume they can get away with it”	J6	1	16
Theme 5: Cyberterrorism Policy Agendas *Category 1*: *Technical Knowledge*			
not enough understanding	E1, C4, P9	4	9(2), 15, 16
shortage of technical knowledge	E1, B2, C4	3	9, 12, 15
complicated technology	P3, A7, P9	3	15, 16, 17
cyberterrorism education	C4, A7	2	8, 9
Category 2: *Policymaker Consciousness*			
immediate threats influencing	P3, J6, A7	3	6, 15, 16
loss of life or capital attention getting	B2, C4	2	15, 16
perception influencing	P3, P9	2	15, 16
making it personal influencing	C4	2	11, 17
public opinion influencing	B2, T5	2	15(2)
inner circle influencing	B2, C4	2	15(2)
reelecting influencing	B2	1	15
press influencing	C4	1	15
received intelligence influencing	T5	1	15
world events influencing	T5	1	17
“didn’t really understand the issue”	P9	1	6
“uneven among industries and sectors”	P9	1	6
“people are still afraid of cyber”	P9	1	6
“don’t pay attention for long”	C4	1	10
“not sought to make cyber a top priority”	E1	1	11
“long-term learning education”	P9	1	15
“leaders who already have a background”	E1	1	16
“senior leaders are less inclined to take on new ideas”	E1	1	17

Code Name	Participants	First Cycle	Interview Questions (times referenced)
Category 3: *Agenda Change Factors*			
policymaker focusing	B2, C4, T5, J6, A7	5	8(2), 14(2), 17
"requires us to rethink our policies"	P9	1	16
"understand what the threats are"	P9	1	16
Theme 6: International Law Considerations *Category 1*: *International Law Validity*			
US must consider international law	E1, B2, P3, C4, T5, J6, P9	11	13(11)
cyber norms and international law	P3, P9	2	9, 13
Category 2: *International Law Integration*			
Russia and China agenda	E1, J6, T8, P9	4	9, 13(3)
China's cyber stance	P3, J6, P9	3	13(3)
two world visions are incongruous	J6, A7	2	9, 13
"continuous instability undermining all the good things"	P9	1	7