5-2020

Asymmetric Threats: Analyzing the Future of Nuclear Terrorism & Cyber Attacks; The Value of Deterrence Theory for Addressing the Challenges of Nuclear Terrorism in the age of 21st Century Cybersecurity

Oliver Demmert-Shelfo
Dominican University of California

Asymmetric Threats: Analyzing the Future of Nuclear Terrorism & Cyber Attacks

The Value of Deterrence Theory for Addressing the Challenges of Nuclear Terrorism in the age of 21st Century Cybersecurity

By
Oliver Demmert-Shelfo

Submitted in Partial Fulfillment of the
Requirements for the Degree of

Bachelor of Arts in Political Science

Department of Political Science & International Studies
Dominican University of California
05/04/20

Table of Contents

Acknowledgments

I would like to thank all of those who provided their support and assistance in the research necessary to complete this Capstone project, including friends, family, advisors, fellow students, and my professors. In particular I would like to thank my thesis adviser Alison Howard for proving guidance and support throughout the writing process. I would also like to thank Dr. Christian Dean for supporting the project in its infancy as well as Dr. Andrew Reddie for providing the initial influence to pursue further work on this topic. In addition, I would like to thank Merit Davey, Adrian Dang, Maria Fernandez, Michael Jones, Renee Martin, Toni McBride, Diana Reidt, and many others for providing additional guidance and support throughout the writing and research process.

Abstract

Given the rapid development and ease of access to technology, the threat of extremist organizations utilizing cyberspace as a means to target critical American strategic infrastructure is of increasing concern. The risk posed by the acquisition of fissile material, sabotage, or use of a nuclear device by an extremist organization has been exasperated due to technological development outpacing strategy. Despite policy-makers' attempts to protect the public from cyber-attacks and nuclear terrorism, the federal policies in place have failed to account for the continual evolution of technology and the gaps in security that this advancement brings. Through examining documents from congressional and bureaucratic agencies using content analysis, this study examines whether or not policymakers, congressional or bureaucratic, use deterrence theory when they make policy, suggestions, rules, and guidelines. This thesis asks how U.S. policy regarding nuclear terrorism has changed given a rise in cyberthreats? This thesis also asks a second question: Which federal agency is most capable of dealing with cyberthreats concerning nuclear terrorism? The findings of this research concluded that as cyberthreats continued to develop, policymakers using deterrence theory shifted to using previous waves of deterrence theory, primarily dealing with rivalry and competitive threats. In addition, this research finds that intelligence agencies are the most capable federal agencies in proving guidelines and informing future policymakers.

Introduction

Prior to 1995, the concept of a terrorist organization gaining hold of and using a nuclear device was based entirely within the theories of early nuclear security academics, military strategists, and in the ideas portrayed in popular novels and films. However, in 1995 this changed when a nerve-gas similar to sarin was used to attack Tokyo's subways, killing 13, seriously injuring 54, and affecting anywhere from estimates of 980 to 6,000 other civilians, (Murakami, 2001). This attack was committed by Aum Shinrikyo, a Japanese cult centered on the concept of a nuclear apocalypse. Prior to the 1995 attack, Aum Shinrikyo had planned to buy a nuclear weapon, and later, as this failed, sought to purchase fissile material from an Australian mine, in which they became suspect. With plans to manufacture their own fissile material, this was scrapped as they felt the perceived pressure of authorities hunting them, instead opting to use a nerve agent. In truth, the authorities were not close to raiding Aum Shinrikyo because of its protection status as a religious group. Only once the attack had occurred and responsibility claimed by the nuclear-zealous cult, did authorities fully learn the extent and efforts made to commit a nuclear terrorism attack. The group had amassed over a billion dollars in bank accounts, operated an Australian farm where it practiced gassing sheep, owned a twelve-acre chemical weapons factory, and claimed sixty thousand followers around the globe (Allison, 2004). After the sharing of information between Japanese and American authorities, the Central Intelligence Agency (CIA) reported to the U.S. Senate Governmental Affairs Permanent Subcommittee on Investigations that the name of the group did not appear on any intelligence agency's lists (Allison, 2004).

Given a rapidly growing proliferation of faster and more capable computing abilities globally, the ability to use cyber warfare as an irregular method for financing operations, gathering information, and performing attacks while maintaining anonymity, is a cost-effective ability many terrorist organizations seek to acquire. The relevance for terrorist organizations seeking to use such technology against U.S. assets has steadily increased over the last few decades. Similarly, the amount of non-state actors and designated terrorist organizations seeking to acquire fissile material, or nuclear weapons, has increased. Among this trend is a growing concern that the security of nuclear facilities and existing layers of countermeasures to prevent nuclear terrorism have the potential to be circumvented or weakened through the use of cyberspace.

There has been a growing amount of cyber threats and cyber warfare capabilities from nation states, terrorist organizations, and even regular criminals, of which current policy and regulations are not informed of and not capable of dealing with effectively. The increase in these threats requires revisiting the effectiveness of policy and determining which federal policy-makers are best able to protect against the threat of nuclear terrorism given new vulnerabilities in the 21st century from the cyber realm.

This paper seeks to answer two questions, filling the gaps in literature on how policy-makers are influenced by emerging threats and provide an update on the roles and responsibilities of federal agencies. First, how has U.S. policy regarding nuclear terrorism changed given a rise in cyberthreats? And, second, what federal agency is most capable of dealing with cyberthreats regarding nuclear terrorism? Answering these questions would contribute to the field of political science by addressing gaps in literature regarding the policy-making process of strategic security issues including nuclear

security, cybersecurity, and terrorism. To answer these questions, content analysis of congressional and executive documents on nuclear terrorism and cybersecurity were used. Using deterrence theory this thesis examines how U.S. policy has changed within federal institutions. This paper additionally addresses the ability of different federal agencies in their application or use of deterrence theory, including the ability for federal agencies to better inform U.S. policy produced by both congressional and bureaucratic agencies. Agencies are also evaluated in terms of their ability to address technological innovation and developments in the cyber realm in order to inform whether or not particular agencies are better suited to deal with cyber threats. Lastly, this paper concludes which federal agencies are the most forward-looking and most informed to be able to inform effective policy to meet the cybersecurity demands of the 21st century. The primary argument proposed is that as deterrence theory has evolved, so too has its use by policy-makers and the resulting policy it informs. In addressing the second question of identifying the most effective federal agency to deal with the future implementation of policies, this thesis argues that intelligence agencies necessitate a larger role in the policy-making process, as they possess the most relevant understandings and expertise of upcoming technological development and emerging threats to inform a more proactive approach to policy, while maintaining intelligence necessary to the successful performance of more reactive inter-agency policies.

Background information is necessary for providing context for the content and research of this thesis. This includes the origins and history of nuclear terrorism as a threat and what cyber threats presently exist or are upcoming. The landscape of relevant academic literature from five fields are reviewed. These include the development of

deterrence theory, 4th wave deterrence as it is applied to both subjects of nuclear terrorism and cybersecurity, the skepticism movement within deterrence theory academia, a review of congressional and bureaucratic policy-making, and addressing the gap in literature that this paper will seek to fill. Following this, content analysis of 18 documents spanning between 1957 and 2018, including congressional hearings, executive statements, reports, reviews will be examined, using deterrence theory as the framework to address how U.S. policy regarding nuclear security has changed with an increase in cyber threats. These documents were examined again, using content analysis, to determine the best equipped agencies to tackle the future of the asymmetric threats of cyber and nuclear terrorism, and ultimately answer the two primary questions that drive this thesis and support the argument presented.

Background & Key Terms

In order to have better knowledge of the context and understandings of the content of this thesis, it is important to address the key terms of nuclear terrorism and cyber threats, and what parameters exist within each of them for the purposes of this paper. The concept of nuclear terrorism, or the use of nuclear weapons by a terrorist organization, has varied in defining criteria in policy and academia. According to a 2016 report the three events that consolidate the study of nuclear terrorism is the buying, stealing, or construction of a nuclear weapon, the use of a dirty bomb utilizing radiological matter, or the sabotage of nuclear facilities (Bun, 2016; Eaves, 2018). This will be the criteria in which nuclear terrorism is looked at as a threat. Although cybersecurity and information security are often used interchangeably, the concept of cybersecurity goes beyond the traditional realm of looking at protecting resources and

data affiliated with institutions, corporations, and governments. Rather, it addresses humans as potential targets as well as other assets that can be manipulated or controlled electronically (Solms, 2013).

Types of Cyber Threats

Cyber threats and their impacts are not widely understood by the general public and can come in various shapes and sizes, utilizing different tactics and dependencies to attack a target. There are three distinct categories of cyber threats, all of which can target consumers to entire government and defense systems depending upon the type and scale of the attack. These include Phishing, Malware, and other new or hybrid threats, including a variety of traditional and upcoming technological developments and attack methods that do not necessarily fit into the other sections or function as a collective.

Cyber threats such as phishing are an increasingly popular tool used against consumers. Phishing can be utilized in multiple ways to fit supporting a nuclear terrorism agenda. Phishing utilizes social engineering, often by establishing trust over time or posing as another ranking official with key targeted personnel or individuals. These attacks are normally executed by having a targeted individual receive a link through email, or text, that they believe to be legitimate, but actually contains a variety of malicious software. This software could be used to hold systems hostage for ransom, persuade employees to make irregular alterations that they believe to be legitimate, install malware, or reveal sensitive information, This attack is common at the consumer level in identity theft and monetary transfers, and is also commonly used to access government facilities by targeting key personnel, allowing for a doorway to future attacks against an agency or layer of security. This usually is the first step in an Advanced Persistent Threat

or APT attack, involving the installation of malware, or monitoring software, that can remain dormant or undetectable for an extended period. This is a favorable method of cyberwarfare by nation states and state-backed organizations, including known terrorist groups (Bonn, 2015). Phishing acts essentially as providing a gateway to future attacks.

The second category of cyber threat that exists in both the consumer and government world is that of Malware. Malware is similar to software in that it can maintain a dormant state to avoid initial detection or slowly eat away at the integrity of a system. It does not require permission to be installed and can serve a variety of functions, including taking control or monitoring actions of a computer system. Malware differs from software in that it has the capacity to be deployed into a singular computer system that can be initially infected, however move throughout a connected network to further systems, able to spread rapidly without detection. Ransomware is a form of malware that restricts access to a user's system, with threats of making data public or deleting it unless financial or political demands are met. Another variation of malware is the Trojan Horse, in which, as the name suggests, the malware is disguised as a piece of legitimate or popular software that is unknowingly functioning to compromise its target (Brenner, 2009).

The third category of cyber threats varies in its applications and threat perception, but includes some of the most commonly utilized threats by terrorist organizations, as well as some of the most sought after upcoming cyber capabilities. Denial of Service (DoS) or Distributed Denial of Service (DDoS) is a method of cyber-attack that is executed by sending an abundant amount of traffic or information, causing the targeted system or service to freeze, and result in not being able to be used. This has been

commonly employed to target consumers as well as the general public and has also been used extensively against government websites and entire state infrastructures to deny critical services, or actions, from being able to take place (Edelman, 2019). Eavesdropping is a form of attack that allows access to key information through intercepting unsecure signals used to communicate between systems or devices or breaking an encryption to do so. In the context of Nuclear Security, compromising Nuclear Command and Control and Communications (NC3) is the primary case in which this may be employed (Futter, 2016; Futter, 2018; Dye 2019). Password attacks are the data variant of Eavesdropping, focusing on decrypting login information in order to legitimately access systems. Man-in-the-Middle (MitM) is a common form of attack in which an attacker is able to monitor, control, or alter the flow of information between individuals and systems, a cyber threat that allows for two or more legitimate personnel to potentially be led to act in favor of an aggressor's agenda. An Insider threat is a cyber threat in which an individual or employee who has legitimate access to a computer system, network, or server installs malware to sabotage systems they have been granted access to. These are particularly damaging as the individual may be aware of the network structure and policies of the agency they are damaging, allowing for maximum threat while potentially remaining undetected (Jajodia, 2014).

Artificial Intelligence (AI) attacks are attacks featuring an independent malicious attacker deploying to computer systems, infrastructure, and other electronically connected assets, that has the ability to learn and adapt to obstacles to fulfill its mission in engaging a target. This is perhaps most notably known through the deployment of the Stuxnet worm to target Iran's nuclear development program in 2010 by targeting

centrifuges to malfunction during the process of the enrichment of nuclear material (Bunn, 2016). Since Stuxnet, the United States and allied nations have deployed similar AI cyber-attacks against other states. However, this technology is being developed and becoming more acquirable by competing nations and potentially their proxy organizations, representing a serious threat to U.S. infrastructure. Lastly, and perhaps the most forward-looking form of a cyber-attack can be found in the form of quantum computing. Although quantum computing promises untold speeds of data and secure encryption, the technology could also be used harmfully (Edelman, 2019). Previous methods of encryption could be rendered obsolete given the access of this capability to an attacker. This means that previously secure government assets and well protected systems are just as vulnerable as their unsecure consumer counterparts, with particular implications for the majority of U.S. national security systems (Futter, 2016). Quantum computing in the hands of a bad actor could compromise defense systems and layers of security to such an extent that many consider the race to fully incorporating quantum computing to be critical to the securing and maintaining a state's position as a superpower in an ever more technology-dependent social, economic, political, and security environment.

According to a GAO report from 2013, the source of these adversarial threats to cybersecurity are not always terrorists, which it notes "seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information" (U.S. Government Accountability Office, 2013, 5). While cyber threats

could be used by terrorists to directly attack a target or as a means to garner the means to operate, terrorists can also work in tandem, hire, or work for a number of other adversarial threats. These include, bot-network operators, those who control compromised networks and remote systems to perform phishing, malware, and denial-of-service attacks. Criminal groups and organized crime can work to mask terrorist activity or provide a source of funding through various methods of attack and espionage. In addressing hackers, the same report states that "According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage" (U.S. GAO, 2013, 5). Insiders are a threat that is particularly concerning, with infiltration by terrorist organizations possible as well as contractors, disgruntled employees, and poorly trained employees acting as accessible methods of using a pre-established user to access sensitive systems. Individuals can be hired or used by terrorist groups who maintain expertise in phishing, spamming, and authors of malware/spyware who can be used to execute attacks.

Lastly, the report stresses the capabilities of nations as being major adversarial threats to cybersecurity, stating "Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony,

the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern" (U.S. GAO, 2013, 5). The capabilities of nations are problematic as cyberspace allows for a space in which providing proof and effective sanctions barely exists. Although both Russia and China have been known to engage in cyber-attacks against other nations, the operations are largely inter-state military cyber-conflicts or measures of influence. However, countries such as Pakistan or Iran who have cyber capabilities and who have been known to back terrorist organizations as proxy sources could proliferate more cyber capabilities to terrorist organizations. As a result, nation-states could enhance terrorist activity, as a means to put further distance between attacking rivals and having an identifiable cyber trail that can be retaliated against. In addition, this threat establishes the importance of the foundation of transnational norms of cyberspace. However, due to the capability and advantage a cyberspace program maintains, it is unlikely that norms will be a byproduct of international cooperation until either the technology reaches a plateau and is widely accessible, or incites large-scale impacts or conflict that cause citizens to push governments to accountability.

History of Nuclear Terrorism

The first instance in which nuclear terrorism was seriously considered was during the 1986 incident of the disaster that resulted from an engineering failure in a Soviet RBMK reactor, resulting in the infamous Chernobyl incident. Prior to further investigation, the Soviets believed at one point that the explosion that caused the incident was due to a western, or internal, sabotage operation. This would have represented the first case of an attack on a nuclear facility and after the disaster, the damage that a civil facility could cause if sabotaged was fully recognized as a threat to security. With the

dissolution of the former Soviet Union in 1991, concerns were raised of loose fissile material or nuclear weapons being acquired by extremist or militant groups that were otherwise operating in the region freely (Kuperman, 2014). This was the first-time nuclear terrorism was held as a legitimate fear by governments and the public of non-state actors having access to nuclear material or assets, with fear these militant groups may want to utilize a nuclear device to bargain for legitimacy. The governments from former Soviet states as well as members of NATO collectively secured and maintained control over nuclear material in the region in a joint effort many in nuclear security and non-proliferation studies to be a great success story (Allison, 2004). This changed however in 1995, when a nerve-gas attack on Tokyo's subways by Aum Shinrikyo, a Japanese cult believing in the need for a nuclear apocalypse, killed several civilians and injured dozens.

Aum Shinrikyo had planned to buy a nuclear weapon, and later as this plan failed, encountered several barriers to obtaining fissile material. With plans to manufacture their own fissile material, they hurriedly scrapped their plans for a nuclear attack due to a perception of law enforcement getting close to discovering their operations. Psychologically deterred by fear of punishment, instead the group opted to use a home-grown variant of sarin gas. After the attack, the Japanese and American authorities convened, admitting they were not close to raiding Aum Shinrikyo and in fact had only had slight run-ins with Japanese police but were never pursued, largely due to its protection status as a religious group. Only once the attack had occurred and responsibility claimed by the nuclear-zealous cult, did authorities fully learn the extent and efforts made to commit a nuclear terrorism attack. This was followed up in the same

year with Chechen rebels in Russia openly displaying a desire to acquire a nuclear weapon. It is unknown as to whether or not these rebels would use the weapon or use it as a bargain for legitimacy. These incidents represent the start of a growing trend of non-state actors openly displaying their desire to acquire nuclear weapons. Al Qaeda became the third primary organization in which a pursuit for acquiring a nuclear device existed when Usama bin Laden openly read a recorded statement in 2003 in which he threatened to use a nuclear device on western states (Wenger, 2012).

This was later repeated in the early 2010s again. For a short time the Islamic State also sought access to a nuclear device, though this seemed to be less serious as past examples in terms of their commitment as well as it was considered highly probable that the device would be used to secure legitimacy rather than as an actual weapon for achieving their goal of establishing a state or central caliphate (Weiss, 2016). Despite this, the threat of radiological attacks persisted. It is unclear, in 2020, if a resurgence in the Islamic State movement will occur or if this goal will be reiterated with more evident commitment. The security of Pakistan's nuclear arsenal given the instability of the country has been cause for concern. In particular, there is concern that loose nuclear weapons or material could fall into the hands of terrorist organizations, or local insurgent groups, similar to the situation during the fall of the Soviet Union, albeit on a smaller scale (Allison, 2004). Due to the uncooperative nature of North Korea and its presence in illicit markets, a genuine fear exists that given the poor internal stability of the state, North Korea may openly sell fissile material, or weapons components, to terrorist organizations in exchange for more common resources that sanctions have prohibited. With the attack on Iranian centrifuges with the Stuxnet worm discovered in 2010, largely

attributed to a joint U.S.-Israel program, and with the recent Iranian intent to continue nuclear development with the collapse of the Iran Nuclear Deal, the threat of an Iranian proxy force gaining access to nuclear material is a serious consideration. In addition, particularly in the consideration of state-backed terrorist organizations, the resources made available for cyber-attacks on nuclear infrastructure or security systems is of a growing concern that ought to be addressed by new policy and existing agencies. In particular the threat of an attack on critical targets such as civil nuclear facilities, threats against Nuclear Command and Control and Communication (NC3), and the stripping back of existing layers of nuclear security measures such as the employment of nuclear forensics that may allow for easier access or entry of nuclear material, are the primary targets that are at the whims of advances in cyberwarfare employed by non-state actors (Bunn, 2016). Due to the lack of technological understanding and speedy development that outpaces policy-makers, no serious regulation on technological development has a presence in U.S. policy. This gap in U.S. national security policy, particularly as it relates to nuclear terrorism, does not take into account new and upcoming threats from the cyber realm. It is important that past policy be reviewed, new policy implemented, and the roles of policy-makers and implementers reviewed to address these issues in a time-sensitive security environment given the proliferation of advancing technology to non-state actors.

Literature Review

In order to address how U.S. policy concerning nuclear terrorism has changed as a result of an increase in cyberthreats, it is necessary that one understands the chronology of literature with respect to the development of information in the fields of nuclear security, cybersecurity, and terrorism studies. Literature regarding deterrence theory and its relationship with these three topics will all be reviewed, following a chronology of the

progression of each wave and related school of thought. The study of these periods is integral for understanding how they can best be combined and applied to addressing the development of policy addressing cyber threats posed by terrorist organizations to nuclear security.

Deterrence Theory

The landscape of literature regarding strategic national security issues most consistently invokes the use of deterrence theory, a theory that holds the most consistent relevance in all three domains of policy regarding the issues of nuclear security, cybersecurity, and terrorism studies. Deterrence theory is a theory by which an actor can deter another actor from performing actions deemed harmful, through the threat of retaliation or repercussions. Deterrence theory was originally developed as a theoretical approach to penology, focused on the psychology of criminals and preventing crime (Jervis, 1985). Since its initial inception, however, deterrence theory has evolved into providing approaches to larger strategic and military applications, laying out the concept that modern military strategy is more so the effective employment of coercion and intimidation in order to prevent a larger break out of conflict or violence as opposed to the traditional sciences of military victory (Schelling, 1966). In addition, Schelling established that nuclear weapons are best used as a deterrent rather than a military solution. This larger doctrine, now known as rational deterrence theory, has its roots regarding nuclear assets and addressing the future of nuclear policy (Knopf, 2010). Taking hold of academia and informing generations of policy-makers, four identifiable waves of deterrence theory have come about. The redefining of deterrence theory took several decades and was ultimately the result of the first three waves until reaching its

modern contextualization within the fourth wave (Schelling, 1966). What would later become known as the first wave of deterrence theory began in 1945.

The first wave is a direct response to the development of nuclear weapons and their impacts on military strategy. Reevaluating the practice of warfare, particularly of an inter-state variety, given the rise of nuclear devices was the paramount focus of this first wave (Brodie, 1946; Morgenstern, 1959). First wave academics believed that they needed to develop criteria for when nuclear weapons ought to be utilized and when their devastation should be considered militarily. This shifted to the potential of using public knowledge of capability and using nuclear weapons as a threat to coerce other states not to enter rivalry. The majority of this theoretical approach was focused on the psychological impact that a nuclear device can have on a potential adversary, given the public knowledge of the destruction caused by such a device. It was believed that the scale of destruction and public understanding would deter adversaries from attacking or becoming hostile with the United States. This first wave of early academics, such as Brodie and Morgenstern, among a variety of other early theorists most notably laid the groundwork for considerations and the future of deterrence theory. Despite this, a limited impact on the practice of policymakers and international relations would cause deterrence not to be approached for several years (Wenger, 2012).

Given the recognition of the preemptive attempts at solutions made in the first wave, the second wave occurred in 1947 when the former Soviet Union became the first nuclear rival, kicking off the second wave of deterrence theory with a more centralized focus among policymakers and preceding academia, the total aversion of nuclear conflict (Wenger, 2012). The failures of the first wave of deterrence to address proliferation of

nuclear weapons and a lack of use in practice led to a more practically driven approach to deterrence, acknowledging that the aversion of conflict was paramount to the survival of the United States. The second wave consisted of a reaction to the great shifts in international relations given the beginning of the Cold War, the focus being on managing nuclear rivalry. It is in this wave that the majority of modern principles of deterrence theory begin to appear. This new wave of deterrence theory quickly evolved to deal with managing nuclear rivalry via the implementation of game theory methodologies (Wenger, 2012). This second wave of deterrence theory is most notable for its heavy dependence on rational choice theory and use of modeling. Prerequisites were established for successful implementation of deterrence in policy: commitment, communication, capability, credibility, and resolve (Kaufmann, 1956). Each of these pillars were expanded on by varying academics to form the foundational roots by which further progressions in deterrence literature would be guided by. Deterrence theory expanded rapidly to include multiple interpretations and classifications.

The second wave is a highlight in the development of deterrence theory through the nuance granted with expansion. Particular applications of practicing deterrence theory were further subcategorized, leading to more specific and varied branches of deterrence theory in academia. The first of these variations is immediate deterrence, where a rival thinks of attacking another actor and the actor responds with a retaliating threat (Morgan, 2003). This is differentiated from the use of general deterrence, where rivals use coercion, often through policy or politics, to regulate threats in a much broader manner (Morgan, 2003). Direct deterrence is the protection of one's own country from a hostile (Kahn, 1960). Extended deterrence is the focus of protecting attacks against nation-states

in which a country has formed an alliance (Russett, 1963). Lastly, there were two variations in targeting methods when applying deterrence theory, countervalue targeting being focused on threatening economic, social, or political assets whereas counterforce targeting were threats against military infrastructure and capabilities (Huth, 1990). Given a rise in use and shifts in interpretation, deterrence was reinforced as a method of making a threat not commit an action, while "compellence" is making a hostile perform a desired action they would not have otherwise (Schelling, 1966). Deterrence by means of punishment, a method of employing threats of action to manipulate behavior became a subdivision of deterrence by denial, a method in which the utility calculus of an adversary is manipulated to lower the perception of benefits a hostile may identify if committing a particular action (Snyder, 1961; Mearsheimer, 1983). These are two distinctions of impacting the utilitarian psychology of a potential hostile through different methods of adding a cost to committing an act or subtracting a perceived benefit. The largely theoretical approach to deterrence theory in this second wave netted results primarily centered on the bipolar state of international affairs given the rivalry between the United States and the former Soviet Union. The goals and assumptions of the second wave were based on maintaining the then status quo of nuclear rivalry, assuming that actors were rational and unitary, a byproduct of its limited application only in the domain of international relations.

Although deterrence theory persisted as a doctrine of nuclear rivalry dealing with nation-states, a third wave of deterrence theory originated during the early 1970s, with the introduction of quantitative and qualitative methods. This empirically driven wave sought to test the theoretical frameworks established within the preceding wave,

including the models, perceived connections, and foundations (Russett, 1963; Morgan, 2003; George, 1974; Snyder, 1961).

Through the qualitative and quantitative testing of deterrence theory, understanding an actor's individual motive was identified as an important part of the new line of deterrence research. The analysis of deterrence either failing or succeeding appeared to be tied to an actor's commitment to an action as well as the cost-analysis by the actor of accepting a threat (Huth, 1984; Salmon, 1976). The third wave began a shift of looking at individuals and delved deeper into the root theories behind the development of deterrence including utilitarianism and rational choice theory. It is here that the concepts of individual actors obtaining nuclear capability is first considered in academia. Given the context of individual actors, the third wave emphasized that an individual actor must be analyzed alongside their objectives and what risks are associated with obtaining the individual's objectives. In this wave, applying utility calculus as well as incorporating human psychology, culture, perceived reactions, fatigue, and how human limitations could impact decision-making were addressed as key functions to understanding how to successfully apply deterrence (Steinbruner, 1976; Jervis, 2003; Harvey, 1998; Walt, 1999; Berejikian, 2002). The inclusion of rewards alongside established threats was reintroduced into deterrence theory from its early penology roots (Huth). It was made concretely clear through quantitative and qualitative evidence that even if utility calculus was applied, utility could be measured and perceived differently by different actors, including those who are deemed rational (Lebow, 1989).

Through the qualitative and quantitative analysis done on the work in the preceding wave, it was determined that the value of positive rewards had been

overlooked by second wave theorists (Russett, 1963). In addition, the assessment of costs from the adversary's perspective could lead to the failings of deterrence theory, as rational becomes subjective, causing breakdowns in previous rational choice approaches to deterrence (Jervis, 1985). Ultimately, this third wave of deterrence, particularly driven by the likes of Jervis, Russett, Lebow, and Stein, produced a more well-defined subcategorization of deterrence theory in practice, focusing on addressing the limitations, interpretations, and assumptions made within the second wave. This qualitative and quantitative-driven period of research would help inform policy-makers and future academics on how to put deterrence into policy and practice, given supportive data for the criteria of success and failure, while introducing the importance of social behavior and individual actors.

The fourth wave of deterrence is considered to be the modern-day application of deterrence theory (Knopf, 2008). Starting after the fall of the USSR and applying the previous methods and understandings made in the third wave, the fourth wave of deterrence is focused on the rise of more asymmetrical threats such as rogue states, cyberwarfare, and terrorist organizations (Smith, 2006; Wyn, 2004; Harknett, 2010; Jervis, 2003; Lebovic, 2007; Libicki, 2009). Due to the relatively rapid growth in non-state actor threats, this fourth wave of deterrence research is in a similar position as the second wave, in which academics have a variety of theoretical approaches, however do not yet possess the empirical evidence to support, properly test, and implement theory into practice (Davis, 2002; Crenshaw, 2003; Wyn, 2004; Wilner, 2011). This fourth wave represents the most current academic deterrence research.

4th Wave Deterrence in Nuclear Terrorism & Cybersecurity

Because the 4th wave of deterrence includes a broader set of actors than previous waves, the primary focus of literature as it relates to this thesis is literature regarding nuclear terrorism, cybersecurity, and general literature regarding non-state actors, in particularly in response to terrorist organizations. Literature on the topic of Nuclear Terrorism or WMD Terrorism is a niche field in which not many academics were previously involved in during the earlier waves of deterrence applications. The introduction of terrorism to nuclear security can be seen in the empirical and evaluation qualities of the third wave of deterrence theory, with non-state actors being addressed in theory sparingly in preceding waves (George, 1974). Graham Allison, a seminal figure in nuclear terrorism academia, led the further development of literature on nuclear terrorism through his comprehensive research in which he details historical context to how non-actors have sought to control nuclear assets in the past and how they may do so in the future (Allison, 2004). Addressing the topic of Nuclear Terrorism, Allison illustrates the reality of a possible nuclear attack by a terrorist organization and how to prevent it from occurring. Brian Michael Jenkins, is a leading figure on understanding the utility and risk calculations a terrorist organization may interpret when considering the obtainment of a nuclear device and in understanding how these organizations value these devices (Davis, 2002). This work in understanding the psychology behind actors pursuing nuclear terrorism and the goal of its prevention is primarily premised on the concepts of deterrence. Martha Crenshaw is another leading figure in the literature on nuclear terrorism, addressing U.S. policy and strategy in deterring al Qaeda from pursing the use of nuclear weapons. She describes the objective of current U.S. policy being the use of deterrence through applying the pressure of retaliatory threats (Crenshaw, 2017).

Through evaluating the Bush and Obama administrations use of strategic deterrence applied to terrorist organizations, policy does not yet fully integrate deterrence theory in addressing a way to effectively achieve nuclear deterrence with terrorist organizations, despite successes in writing policy, the practice and implementation has several failings (Crenshaw, 2017). Overall, literature on nuclear terrorism is largely derived from theory surrounding the cases of non-state actors who actively sought or pursued interest in accessing nuclear material or assets. This has led to the expansion of a fields involved in addressing nuclear terrorism, with attempts at producing practical responses for a variety of fields including medicine and sciences, given the potential for a future attack (Auerswald, 2006; Knopf, 2010; Dunn, 2008). This has widened the literature in nuclear forensics, believing to act as yet another deterrent to proliferation or movement of nuclear material by terrorist organizations (Knopf, 2008). Despite dealing with terrorist groups as actors and rogue states as suppliers, the increase in rogue states has led to a higher probability of state-backed terror groups, who would have more support than traditional terrorist groups (Knopf, 2010).

When applying deterrence to the realm of cyberspace, academia is clearly within the confines of the fourth wave of deterrence theory development, however appears as though it were the first or second wave. The rise in technological reliance and capabilities in conjunction with the rise in cyber threats and state-sponsored cyberwarfare have brought academics to rush into creating new theoretical approaches at dealing with the rise in virtual threats. In terms of deterrence theory's applications to cyberspace in academia, they are twofold. One, because of the successes in other realms of security issues and its various methodologies of employment, deterrence theory is best suited to

deal with the issues presented by cyber threats as the principles of utility calculus and non-state actors in the fourth wave clearly show that cyberspace is another asymmetric threat (Heitzenrater, 2015). In addition, the fast pace of technological development doesn't leave much room for the adoption of entirely new methods of approaching security policy without leaving a further compromised position in cyberspace. This can be remedied via the further development of cyber-deterrence theory (Kramer, 2013; Dogrul, 2011). Secondly, deterrence theory in the fourth wave suffers in many of the same ways as the second wave in that there is a lack of empirical evidence that employing deterrence is effective or worthwhile (Taddeo, 2018). In addition, the underlying assumptions that deterrence in cybersecurity issues would work in the same way as when applied to terrorism studies is in question (Harknett, 2010). In addition, the study of cyber-deterrence suffers from a lack of an effective game model as in classical deterrence theory approaches due to the non-existence of clear preceding rules and regulations in cyberspace as there had been during the second wave of deterrence as applied to nuclear weapons (Bendiek, 2015; Stevens, 2012). Despite this, the cyber domain is internationally recognized as the next frontier of conflict (Osawa, 2017).

Skepticism in Deterrence Studies

Although deterrence theory and its waves are the dominant school of thought given the three topics of nuclear security, cybersecurity, and terrorism in terms of applied theories, another category of academic literature exists. This is skepticism, a self-analytic approach in which literature is reviewed and critiqued given changes in academia, data collection, and shifts in agency policies. Skepticism functions largely as the nuclear-specific equivalent of the self-criticism school of thought available in the broader scope

of terrorism studies and serves in the same manner for cybersecurity academia. This method often looks at establishing assumptions made within larger theories, dissecting whether these assumptions are true or effective given new data or academic revelations. The rise of the third wave of deterrence theory, bringing its psychological roots and further data collection, is largely responsible for the increase in skeptic scholars, in which classic assumptions and premises for the successful use of deterrence theory have fallen under scrutiny. Among this scrutiny have been calls for changes in how deterrence theory ought to operate and inform policy-makers in the future, questions whether deterrence theory is still relevant, and what limitations it possesses. A contention with deterrence theory that skeptic scholars have focused on in recent years is the case of acquisition-use theory. Acquisition-use theory is a theory that takes into account the premises of deterrence theory in terms of employing utilitarian calculus and rational choice theory in order to come to the conclusion if a terrorist organization would or would not use a nuclear device if one was obtained (Bell, 2019). The application of game model theories that have previously been employed in past nuclear literature are a particular target of skeptic review, given that perceived conclusions of data as well as the implications for the interpretations of what the data collected means, fall under scrutiny here such as in the case of threat analysis inflation. (Lewis, 2002; Colbourn, 2015). This inflation would drastically alter the presented likelihood of an event, particularly in regards to attacks, with such subjectivity that the data presented to policy-makers has been deemed unreliable in later review. In this way, skepticism is used to help understand how interpretations of the work in deterrence theory literature can vary, and how this variation

can drastically alter the policy and policy-makers work in deterrence theory seeks to inform.

Policy-Makers: Congress & Federal Bureaucracy

In attempting to understand how U.S. policy regarding nuclear terrorism has changed as a result of an increase in cyber threats, it is important to understand the policy-makers that will ultimately be responsible for putting theory into practice. The most relevant U.S. policy can be split into two categories: Congressional and Bureaucratic. Congressional policy and Presidential statements on nuclear terrorism as well as bureaucratic agency reports and reviews have been the primary employers of deterrence theory in policy. However, the historical practice of these policies has not netted the desired results initially sought in writing (Crenshaw, 2017). As a result, the implementation of policy has been increasingly deferred among agencies to others with specific knowledge or capabilities, such as intelligence agencies, law enforcement, and defense institutions, who are better equipped to carry out specific tasks needed for the enforcement of policies. This diffusion of responsibility is not intentional in policy, however could occur due to a potential lack of understanding and capability of different agencies by policymakers when deciding on agencies best fit to implement policy. In addition, a selected agency could seek out additional support from another with more assets or intelligence on accomplishing a specific policy goal so repeatedly that a de facto state of responsibility exists but is by no way guaranteed. Despite this, congressional policy has slowly started making the shift of addressing policy, along with the division of responsibilities among bureaucratic agencies, focusing on non-state actors as it applies to nuclear security and applying deterrence theory (Pandza, 2011).

The internal policies produced by bureaucratic agencies, or the additions built on by congressional guidelines are more detailed and accurate to modern trends; however, the various realms in which each of the federal agencies operate and have jurisdiction has created conflict in the execution of policy. In addition, inter-agency cooperation has continued to be an issue that hampers the development of further cyber-deterrence policy in regards to nuclear terrorism (Harknett, 2010). This inter-agency conflict was addressed by the Obama Administration in a review of Homeland Security policy. As these agencies have the most accurate information and understanding of both nuclear and cyber assets, it is recognized by some academics that some of the successful implementations of deterrence theory found in past agency policy can be applied in the future (Nye, 2011). Bureaucratic agencies are also considered to be more effective and influential due to their overall better prioritization on security issues compared to that of Congress (Nye, 2013). In addition, these agencies have particular expertise associated with their particular mission set that are necessary when addressing highly technical or complex security issues, something that Congress lacks. The increasing reliance on bureaucratic agencies has also introduced more proactive deterrence theory tactics into execution, giving agencies a method of working more proactively at implementation than congressional policy addresses (Oti, 2015).

Given the current landscape of literature and academia, the issue this thesis seeks to address is a representation of combined features of the fields of nuclear security, cybersecurity, and terrorism studies through the context of the policy-making process. Each of these fields of study have their own varying uses of deterrence theory, this thesis is uniquely incorporating all three, whereas these issue areas would be addressed in pairs,

or singularly, in the status quo of academia. This led to two primary research questions being developed. How has U.S. policy regarding nuclear terrorism changed as a result of an increase in cyber threats? What federal agency is most capable of dealing with cyberthreats concerning nuclear terrorism? In answering this first question, understanding the development of deterrence theory as applied to all three issue areas collectively, this paper seeks to argue that as deterrence theory has evolved, so too has nuclear security policy. This change will inform the content of the policy as well as provide guidelines for bureaucratic agencies, leading to the second question. Given superior intelligence resources and ability to respond to threats more directly, this paper argues that intelligence agencies are in the best position to deal with cyberthreats concerning nuclear terrorism.

The pursual of these research questions fills a significant gap in nuclear terrorism literature. In existing nuclear terrorism academia, cyberthreats are most often given the context of traditional deterrence theory between rival states as opposed to non-state actors. In existing cybersecurity literature, the vulnerabilities of nuclear systems represent a niche of literature, similarly contributing to inter-state conflict rather than terrorist organizations or individual actors. In terms of terrorism studies, literature exists on both cybersecurity and nuclear issues, however end in pairings. This contribution to the academic field of political science is unique in its focus on all three issue areas collectively. The results of this study contribute to the fourth wave of deterrence theory in assessing how asymmetric threats inform deterrence theory and in turn impact decisions for policy-makers and ensuing policy. Lastly, this study provides more empirical evidence, informing the disconnect between policy and application, identifying which

federal actors are in the best position to extend deterrence theory successfully into the future, perhaps into a fifth wave.

Theoretical Framework

The primary theoretical framework for the study of this paper is deterrence theory. Deterrence theory is the dominant theoretical approach that informs policy-makers and leadership in a variety of issue areas including nuclear security, cybersecurity, terrorism studies, and military strategy. The theory derives from a psychological theory of the same name, commonly applied to the study of penology and criminal law. In its psychology and criminal basis, the theory is used in two parts in order to achieve a desired outcome. First, the threat of punishment will dissuade or deter an individual from committing a crime again. Secondly, the public knowledge of this punishment is psychologically stressing enough to deter individuals from committing the crime in the first place. Its application then shifted to addressing the future of military strategy and the development of nuclear weapons (Schelling, 1966). Although deterrence has gone through a variety of changes in its four waves of application, primarily to nuclear issues, this study applies the use of fourth wave deterrence theory to examine how U.S. policy regarding nuclear terrorism has changed with an increase in cyber threats.

Fourth-wave deterrence theory in particular looks at the application of deterrence to asymmetric threats. This includes non-state actors, individuals, terrorist organizations, rogue states, and upcoming threats (Smith, 2006). This fits primarily with the first research question. How has U.S. policy concerning nuclear terrorism changed with an increase in cyber threats? This question incorporates the asymmetry of terrorist

organizations and cyberspace with the modernization of the theory in regards to nuclear security.

Deterrence theory incorporates several other theoretical approaches as the basis for its operation. Included in this is rational choice theory, an 18th century theory developed by Cesare Beccaria. The premise of rational choice theory lies in that the social collective is made up of individuals, with each individual being able to make choices and preferences when given a variety of options. The individual will take into account public information and understandings about the world around them, informing their desired choice given a situation in which their decision is a variable. This calculation may be done over time regarding large decisions, however could often be used to understand why individuals perform seemingly mundane tasks a particular way. The driver behind this could be described as utility.

This leads into yet another foundation of deterrence theory in the form of Utilitarianism. Developed into literature by Jeremy Bentham, but not necessarily its first instance of understanding, utilitarianism can be described as a method in which an individual will attempt to maximize their own utility, with utility being subject to variation but generally related to the prospect of increasing pleasures, advantages, happiness, and other positive interpretations of an individual gaining something. In addition, it references the prospect of utility excluding negative connotations. This core principle of utility can be used broadly or redefined to specific issue areas, in this case security, safety, and continual existence are recurring interpretations in literature on nuclear terrorism. This inherently is a core principle in rational-choice theory as it is

applied to deterrence and in game modeling, often acquainted with early phases of deterrence.

Data Collection/Methodology

To answer the research question of how has U.S. policy concerning nuclear terrorism changed as a result of an increase in cyber threats, content analysis of documents pertaining to nuclear security, terrorism, and cybersecurity was analyzed. Given that the text of documents is being analyzed and the research questions asked by this thesis, content analysis was the best methodology to use. Content analysis is a methodology defined as making objective inferences and identifying, systematically, particular characteristics in a text (Holsti, 1969). The eighteen texts studied for this project span from 1957 to late 2018 and include: thirteen Congressional hearings from both the House and Senate, more specifically from the Committee on Homeland Security, Committee on Armed Services, Committee on Foreign Affairs, Committee on Foreign Relations, and the Committee of Governmental Affairs; a review conducted by the Government Accountability Office (GAO) in February of 2013, a presidential advisory committee report from late 1957, and three national strategy statements by two White House administrations from 2003 and 2018.

Using content analysis, these documents were coded for a variety of elements (See Appendix A). Along with basic identifying information regarding the context of the document such as the title, year produced, agency, subcommittee; each document was coded for the asset, infrastructure, or system of concern that is under threat and being addressed, as well as the non-state actor being perceived as threatening. Following this, the type of cyber threat was coded for, if one is addressed. Each of these types of threats

were quantified with regards to how many times they are mentioned. The content and context of addressing the cyber threat were recorded. Several other factors were coded for pertaining to each document, with a yes or no answer. These other factors include: whether or not the document addresses future or upcoming threats, whether or not the document provides guidelines to bureaucratic agencies on enforcement or implementation, and whether or not the document references previous policies, noting if the referenced policy was perceived as negative or positive with the unit of analysis being individual words, sentences, and paragraphs. In addition, the documents were also coded for the specific method for employing deterrence, what the intended target is for being deterred, be it individuals, groups, assets, and others; whether or not the deterrence used is limited to direct deterrence, as it is dealing solely with the United States (Kahn), or extended, dealing with allies. Being the sole coder for this study, there is no intercoder reliability.

In answering the second research question of what federal agency is most capable of dealing with cyber threats concerning nuclear security, several additional factors were coded for. Again, content analysis was used to quantify and log how many times a particular federal agency was mentioned explicitly or implicitly, as well as particular departments that may be part of a larger agency. Through this coding process, the research shows what agencies are critical to filling the gap in providing an effective defense against nuclear terrorism in the age of 21st century cybersecurity.

Findings/Analysis

The use of deterrence theory by policy-makers to inform policy and decision-making within federal agencies in addressing nuclear terrorism as well as cyberthreats

has been consistent. Although the use of 4th wave deterrence theory is inherent in addressing these asymmetrical threats, it is clear from an analysis of the documents examined for this thesis that policy-makers have not abandoned the second wave of Cold War-era deterrence theory. Second wave deterrence is mostly applied to international relations, when one is dealing with states and rational opponents, rather than rogue states, terrorist organizations, or asymmetric threats that dominate the fourth wave of deterrence theory. Second wave deterrence is a critical component for addressing cyberthreats as nation-states have yet to organize or create rules amongst themselves.

The use of second wave deterrence theory in conjunction with fourth wave deterrence theory to address cyberthreats also represents how cyberthreats have reintroduced concern at the nation-state level in security regarding nuclear terrorism, requiring international cooperation. In addition, this shows that asymmetric threats can also function as traditional second wave rivals, with the capacity to counter or perform attacks with similar efficiency. This counter the points raised by authors like Harknett and Taddeo, who call into question the use of deterrence theory in cybersecurity. Although their concerns are mainly derived from a lack of empirical evidence, the capability that the use of cyber threats offers terrorist organizations creates a more balanced, yet asymmetric security environment with other nations. This showcases a clear need to incorporate second wave deterrence theory alongside fourth wave deterrence theory as the asymmetric threat has developed to a level that it could be used to undermine the advantages held by recognized states, allowing for terrorist organizations to utilize cyber capabilities as a means to enter a rivalry that is protected by their lack of geographic restriction and abilities to operate without rules.

The previous gaps in the security of nuclear-related assets that have been filled have been reopened with the introduction of more complex cyberthreats, including various methods of circumventing nuclear forensic technology used to detect, track, and create a barrier for movement of fissile material, required to use or produce a nuclear device. In addition, the use of artificial intelligence paired with traditional worm-based cyber-attacks have clear implications for the laboratories, civilian power system, and potentially portions of the traditional nuclear triad. This concern has increased since the public acknowledgment of the Stuxnet worm in 2010, with the potential for more advanced artificial intelligence to make future worms more destructive, a threat noted in the 2018 National Cyber Strategy. "The United States Government will examine the use of emerging technologies, such as artificial intelligence and quantum computing, while addressing risks inherent in their use and application" (United States, 2018, 15). The upcoming development of quantum computing has implications internationally as well, creating a situation in which previous encryption and security systems utilized by any government could be compromised. This vulnerability is addressed in the 2018 National Cyber Strategy of the United States of America, stating "To protect against the potential threat of quantum computers being able to break modern public key cryptography, the Department of Commerce, through the National Institute of Standards and Technology (NIST), will continue to solicit, evaluate, and standardize quantum-resistant, public key cryptographic algorithms" (United States, 2018, 8). In terms of an effect on nuclear terrorism, this technology could circumvent the protections used to protect the traditional nuclear triad, previously protected via its lack of connectivity, but potentially leaving NC3 capabilities vulnerable as technological progress creates new avenues for opposition

forces to perform attacks. In the 2018 National Strategy for Countering Weapons of Mass Destruction Terrorism, the introduction of new or novel threats, including those of a cyber nature is of clear concern, stating "The brief span between the discovery of the neutron in 1932 and the use of nuclear weapons in 1945 illustrates the stunning pace with which unexpected threats can materialize. Yet, future WMD threats might arise not only from exotic new capabilities but also from reduced barriers to extant technology. Others may stem from novel combinations of technologies to produce unforeseen effects, a phenomenon foreshadowed by our adversaries' increasingly creative coupling of cyber-attacks with disinformation campaigns" (United States, 2018, 12).

Through these findings, although there has been a significant move forward to using fourth wave deterrence theory by policy-makers, in synchronization with academia post 2001, second wave deterrence has become increasingly used as the complexity and capability of cyberthreats grow (See Figure C). Independently, one could come to the conclusion that if separated from the context of nuclear terrorism, cybersecurity and addressing cyber threats alone seems to follow a similar development cycle in terms of deterrence theory as nuclear security had during its inception in the late 1940s. There seemed to be a significant trend in the movement to second wave deterrence in conjunction with the consistency of the fourth wave deterrence theory as the complexity of a threat grew, or, in other words, as the type of cyber threat had potential to affect multiple nations, establishing cooperative relationships with other nations became a priority. Now nation-states like the United States must look at other nations as rivals as well as non-state actors and rogue nations as more serious threats than previous, capable of rival methods of engagement. This is again represented in deterrence theory with the

most common use being direct deterrence followed by extended deterrence, showing that the focus of the application of deterrence theory among policy-makers is on protecting the U.S. via its own resources, placing cooperation with allies as a secondary priority (See Figure D). This focus is acting in contradiction to Osawa's claims of understanding that cyberspace is the next critical area of operations when it comes to emerging conflict, perhaps showing the reactive nature to policy-makers. In this case, Crenshaw's concerns of implementation could be reinforced due to a lack of up-to-date understanding of cyberthreats held by policy-makers.

In terms of addressing cyberthreats, legislators are clearly reactionary rather than proactive. Following an increase in cyberthreats and the complexity of which is growing, demonstrated by the deployment of Stuxnet in 2010, the Cyber Intelligence Sharing and Protection Act was implemented in 2013. At the time, 2013 and 2014 represented the largest consideration for cyberthreats being addressed by legislators, fifty-five and fifty-two times respectively. This reaction would repeat, with a variety of 2015 hearings producing a previous average of around fifteen times cyberthreats were addressed per document. Following cyberattacks on U.S. election systems in 2016, cyberthreats were addressed ninety-one times, representing a new high, shortly before continuing the previous trend of only being addressed an average of fifteen or so times by legislators per hearing or report. In addition, of these documents, 61.1% addressed future or upcoming threats to security. However, only 33.3% provided guidelines for implementing policy or providing a division of responsibility among agencies, only seeming to do so several years after a peak in concern.

This was reflected in the earliest form of national strategy with the 2003 *National Strategy to Secure Cyberspace*, that provided a list of initiatives and major goals, but did not provide guidelines, delegate responsibility, or provide resources for how to achieve them. This critique of the 2003 strategy was present in a 2013 GAO report, that stated "The lack of milestones and performance measures at the strategic level is mirrored in similar shortcomings within key government programs that are part of the government-wide strategy. For example, the DHS inspector general reported in 2011 that the DHS Cybersecurity and Communications (CS&C) office had not yet developed objective, quantifiable performance measures to determine whether it was meeting its mission to secure cyberspace and protect critical infrastructures" (Government Accountability Office, 2013, pp. 31). This is a concerning trend given that the Department of Homeland Security (DHS) has had the largest growing trend of all other federal agencies since 2003 (See Figure C) with regard to cybersecurity when concerning nuclear terrorism.

In terms of the development of policy, there seems to be a significant amount of review of past policy, with 83.3% of documents reflecting on or referring to past policy. Of this discussion, 33.3% of past policy was seen as positive, 27.8% as negative, 22.2% as discussing past policy both positively and negatively, leaving only three of eighteen documents that neglected to reference previous policy. This shows that along with being reactive in nature, legislators are also attempting to understand how policy has been implemented after previous discussion, showing a disconnect between policy-makers and the implementation of policy as well as a lack of technical knowledge necessary in addressing the issues related to cyberspace and nuclear terrorism. This reactivity over proactivity was identified as early as 2005 by the House of Representatives, which stated

"Better intelligence can be seen as a dynamic component of nuclear defense, complementing the essentially reactive and stationary risk management systems that the United States is implementing" (U.S. House of Representatives, 2005, 8).

It is clear that cyberthreats have the ability to reopen vectors for attacks that were previously thought to be secure. For example, "Since 2009, after President Obama's administration, DNDO (Domestic Nuclear Detection Office) has made important changes and made especially good progress in nuclear forensics" (U.S. House of Representatives, 2014, 4). Along with upcoming or experimental threats, the cybersecurity of nuclear forensics systems was a cause for concern over modern nuclear security, a trend following this 2014 statement. This shows that security must be continually developed as new threats emerge. In regards to addressing nuclear forensics, it was made clear that the least likely method for a direct attack would be on NC3 systems or nuclear triad assets as the physical installations are well protected and in cyberspace are either disconnected in such a way that an insider threat is mandatory or are protected by the technological barrier to entry in regards to the development of complex and expensive computing capabilities. Instead, nuclear forensics are of great concern as it would help track and deter terrorist organizations from moving nuclear material and ultimately alert authorities toward a potential development or deployment of a nuclear device. The primary threat that this technology safeguards against is from rogue states, criminal groups, or other terrorist organizations providing nuclear material or smuggling capabilities to an extremist group. This connects to the bulk of literature coming from the foundations of the 4th wave of deterrence theory.

This acts as the primary effort for deterrence as there is no shortage of fissile material to be used for a nuclear device or "dirty-bomb." For example, the U.S. The House of Representatives Committee on Homeland Security, Subcommittee on the Prevention of Nuclear and Biological Attack stated "Also we cannot rule out the possibility that terrorist organizations may attempt to construct nuclear weapons. Although assembly may be a far more difficult path than theft, considerable dual-use technology continues to become accessible. And whether nuclear power generation expands or contracts in the years ahead, a huge overhang of weapons-usable material will remain as a potential source of nuclear weapons" (U.S. House of Representatives, 2005, 5). By deterring access to nuclear material through detection systems, an attack could be dissuaded. However, cyberthreats on these systems could eliminate or hamper this measure of defense.

Overall, the trends for policy-makers show growing concern for upcoming threats, particularly those that eliminate detection and tracking capabilities, necessary for providing important intelligence to authorities on developments of a terrorist organization's movement of nuclear material or a device. A concern that is supported by Knopf. This can be seen as the agencies responsible for these defensive capabilities are increasingly mentioned by policy-makers (See Figure C). In addition, policy-makers share a growing concern for strategic level cyberthreats that could be employed by nations states and more particularly rogue states that may use an extremist organization as a proxy, providing cyber capability to achieve any measure of military, intelligence, or political advantage over the United States. Because of the relatively new technology that cyberthreats encompass, the use of fourth wave deterrence theory in nuclear terrorism

scenarios by policy-makers continues to show dominance. However, there is a resurgence in second wave deterrence theory as cybersecurity becomes a growing concern (See Figure B). As a result, deterrence theory continues to have important strategic implications for both the realms of nuclear security as well as cybersecurity when dealing with non-state actors, particularly terrorist organizations. Despite calls for the abandonment of deterrence as a theory of practice (Lebow, 1990; Lewis, 2002; Harknett, 2010; Iasiello, 2014; Colbourn, 2015) to inform modern strategy, particularly in regards to the cyber realm, it clearly retains a prominent stance in informing the national strategy of the United States as well as policy-makers. Rather, the introduction and progression of cyber developments could have the potential to support previous assertions of deterrence theory, with potential for further development of 3rd wave deterrence and the introduction of a potential fifth wave, dealing with more modern asymmetrical threats. This is important because third wave deterrence theory will have entirely different critiques regarding cyberthreats than it did with nuclear threats, as the nature of the threat and accompanying policy have key differences. The progression of technology could show that the 4th wave of deterrence is too broad to address cyberspace and future developments within the same category of rogue states and terrorism as it currently does, this could result in the need for a more focused category of deterrence focused on automated threats that lack the influence factors found in heads of state, individuals, and more traditional factors. As a result of the introduction of new technologies and the advent of cyber threats, policy regarding nuclear security has shifted to an increased use of second wave deterrence theory alongside the long-standing status quo of post-9/11 use of fourth wave deterrence theory. As the understanding of cyberthreats continues to grow,

one could expect deterrence theory applied to cybersecurity to independently follow a similar direction of the four waves of nuclear deterrence. The increasing use of second wave deterrence theory show that policy-makers are still primarily focused on controlling rational actors and that the asymmetric nature of these threats cannot be solved without transnational norms and cooperation to establish a baseline on which to defend against threats that are inherent within the fourth wave of deterrence theory.

In addressing which federal agency is best able to deal with cyberthreats to nuclear terrorism, the findings of this study indicate that while DHS continues to have a growing amount of relevancy, particularly with its variety of offices focused on the detection and security of nuclear material and assets through its direct deterrence measures, DHS is becoming increasingly dependent on the findings and information provided by intelligence agencies (CIA, NSA, DIA, FBI). Although DHS and a variety of law enforcement agencies are particularly well suited to dealing with the prosecution and operations side of targeting nuclear terrorism activity, intelligence is necessary to make these operations effective as well as become more preventative than reactionary. The House of Representatives recognized this in 2005 when it stated "Not enough is known about adversaries' WMD procurement networks in nuclear supplier states: how they are organized, and financed, what front companies and other intermediaries are used, who their inside collaborators are and so on" (House of Representatives, 2005, 8). This shows that the roles of intelligence agencies in their information gathering skills as well as their technical expertise in dealing with cyber threats are an important asset that must be utilized further to effectively address upcoming threats. This was reported to the United States Senate in 2008 with the statement that "the IC (Intelligence Community) provides

information critical to our technology development and requirements roadmaps. Additionally, our Nonproliferation R&D program managers and our laboratory researchers hold appropriate security clearances and are well-informed of threat analyses from the IC. We use the results of the threat analysis to guide and steer our investments in R&D to ultimately develop sensors to meet the present and future nonproliferation threat" (United States Senate, 2008, 51). The lack of intelligence-sharing capabilities revealed significant gaps in defense systems, the Senate addressing these gaps in 2008 stating "Some steps taken to close these gaps include the development of the Situational Awareness CWMD Information Portal and the Interagency CWMD Database of Responsibilities, Authorities, and Capabilities to increase coordination" (United States Senate, 2008, 50). Inter-agency cooperation has severely limited the response to cyber-related issues as addressed by the GAO in 2013. "Most of the strategies lacked clearly defined roles and responsibilities for key agencies, such as DHS, DOD (Department of Defense), and OMB (Office of Management and Budget), that contribute substantially to the nation's cybersecurity programs" (Government Accountability Office, 2013, 33). This shows that the issue of inter-agency cooperation is an issue that both nuclear terrorism defense as well as cyber defense have in common.

In 2015, the Obama Administration made an important statement in the White House National Security Strategy of 2015 addressing the lack of cooperation among agencies dealing with these issues. This called for a clearer division of roles and responsibilities. However, this did not influence the majority of the intelligence community in regards to a major shift in cooperation, rather only a natural increase in relevance among other departments as intelligence and expertise on new threats became

apparent to legislators as a high demand factor. Prior to the Obama Administration's statement in 2015 the Intelligence Community Information Technology Enterprise (IC ITE) was developed in 2013, allowing for streamlined information sharing across agencies. Despite this, the lack of agency cooperation was not seriously addressed until after the release of the 2015 National Security Strategy. This further supports Crenshaw's points of failings in the implementation of policy.

Inter-agency cooperation is necessary for an effective defense against cyberthreats and nuclear terrorism. There is a clear trend in an increasing number of agencies dealing with these issues , and, as a result, the expansion of bureaucracy could be a limitation on a proactive response to cybersecurity and nuclear security concerns from terrorist organizations if not informed via proper intelligence and allowing for intelligence to be shared (See Figure C). The inefficiency of the diffusion of responsibility is supported by the findings of Crenshaw in terms of policy implementation and again by Allison where weaknesses in reactive responses reside. This lack of cooperation was highlighted a decade prior to the Obama Administration addressing the issue, where the House of Representatives had addressed the issue, stating "Given the U.S. agencies that are responsible for the programs that compromise a defense in depth and the geographic span of the activities, the nation's efforts to counter nuclear terrorism must be formulated and implemented within an overarching, integrated, global architecture. Given the size and complexity of the endeavor, this architecture must be based on a systematic assessment of risks vs. investments" (U.S. House of Representatives, 2005, 13). This shows that the issue of inter-agency cooperation is not new, and the multi-agency effort must be addressed with multi-agency cooperation. With an increase in terrorist attacks globally

between 2005 and the White House's 2015 statement shows the gaps in cooperation to be detrimental to the security of the United States. While the White House addressed national security particularly in regards to terrorism in 2015, the prospect of Nuclear Terrorism being subject to the same weaknesses was still identified previously. This was clearly identified in 2005 when the House Committee on Homeland Security and Subcommittee on Prevention of Nuclear and Biological Attack stated "But the real key to countering nuclear terrorism is effective coordination among all of the agencies with responsibilities for this exceedingly difficult problem" (U.S. House of Representatives, 2005, 13).

Although there was a clear rise in intelligence agency participation following the 2016 cybersecurity breaches (see Figure C), further involvement of the intelligence community in terms of sharing information with other relevant agencies in a more proactive manner would enable a stronger defense system for addressing cyber threats and nuclear terrorism. The intelligence community is in the best position to complement cyber and nuclear deterrence because of their significantly more advanced technological expertise, necessary for addressing the rapid pace of cyber developments, as well as providing the underpinning intelligence for operations and defense systems to be effective via quantifiable data providing a capability to address milestone reviews. This would enhance proactive defense measures against threats to nuclear and cybersecurity from terrorist organizations and embolden a more well-informed inter-agency process for the application of national strategy using deterrence. Although the deterrence theory in itself does not call for cooperation, due to the lack of transnational norms, cooperation of an internal as well as external nature is necessary for establishing operational intelligence

and guidelines for other agencies to proceed, in the future, effectively in preventing nuclear terrorism and protecting against cyber threats.

Conclusion

Through this research, there is evidence that deterrence theory has a place in the future of strategic U.S. national security among policy-makers. As deterrence has historically and currently continues to inform evolving strategies for a variety of emerging threats, deterrence theory has shown to be capable of adapting to technological advancement. The advancement and proliferation of cyberwarfare capabilities must be addressed in a proactive manner, as terrorist organizations continue to gain more competitive capabilities. With this advancement, the use of deterrence by policy-makers will be critical in formulating effective strategic guidelines in order to protect against cyber threat and nuclear terrorism. While these policy-makers are important in responding to emerging threats, it is equally, if not more so, important that policy-makers possess a full understanding of emerging technology, threats, and the capabilities and resources that are provided by a variety of bureaucratic agencies. This thesis has determined that the federal agencies encompassing the intelligence community are the most capable of guiding and informing policy-makers and other responsible agencies in the chain of implementing both policy and operations supporting the goals of policy-makers.

One of the weaknesses of this study is the number and type of documents reviewed. The sample size for this study was small because of a lack of public department-specific or agency policies that reflect ongoing implementation of relevant federal agencies. As a result, the congressional hearings, GAO report, and executive

strategy statements were necessary for formulating an understanding of the status of nuclear terrorism and cybersecurity through the perspective of legislators. This is a weakness in that although being informed by experts, the legislators themselves still lack a clear understanding of details and emerging threats due to the lack of technical expertise or national security issues being only a subset of legislator responsibilities. This means that while the hearings are important to understanding the policy-making process, the content could be misinformed in comparison to the understandings provided directly from responsible federal bureaucratic agencies. In addition, the policy-making process is slow and through the findings of this thesis, largely responsive, meaning that the accuracy of information to date could be incorrect due to the fast pacing at which technological developments and emerging threats shift. The analysis of this thesis led to the understanding that there is a lack of clear division of responsibility among competing federal agencies, however the inability to address internal agency reports constituted a limitation of the findings of this study. Another weakness in this study was that as the documents became closer to the present day, many critical responses and sections between legislators and agency personnel remain redacted from public record as of the time of conducting the research. The presence of this redaction becomes particularly clear in 2018. In addition, due to the fast pace at which cyber-related developments move, it is unclear that within the two years between the dates of the documents and when this study took place, if policy has become more responsive or proactive. The lack of information/data could have the potential to alter the findings of this study. As information security, or redaction, continues to be a key pillar of nuclear defense, a lack of publicly available information could be a potential sign of further efforts at

maintaining security, however it clearly functions as a limiting factor as to the depth of this study.

As the development of deterrence theory has evolved as nuclear security priorities shifted, one could expect issues involving deterrence and cyberspace to follow a similar trend in evolution. It is clear that deterrence theory still remains a major strategy employed by federal agencies and legislators when tackling cyber threats. Just as deterrence was used to address nuclear security, one could make similar assertions that the use of deterrence theory to address threats from cyberspace will follow a similar progression of establishing transnational norms and dealing with rational actors, with addressing critical gaps and strategies, prior to progressing into dealing with the more asymmetric implications and employers of cyber threats. However, with the asymmetric nature of the threat being employed by an asymmetric force, the use of cyberwarfare by terrorist organizations enables terrorists to maintain a rival capability with established nation-states. This appears to be the trend currently, with the beginnings of a phase two era of deterrence in transnational talks and an increasing occurrence of phase two deterrence appearing in U.S. policy. However, the application of deterrence theory is limited to the speed at which legislators and agencies can produce policy, agreements, and build defenses, a speed that drastically lags behind the progression of technological innovation. Thus, although deterrence has shown to be successful to address nuclear issues, the prospect of a lack of success in its application to cybersecurity seems to have less to do with the lack of deterrence as a viable strategy and more to do with the status-quo pacing of building and developing solutions through policy-makers and distributing these solutions across multiple agencies. As a result, deterrence theory is still valuable in

addressing cyber threats, and in particularly their extension of threats to other areas, such as nuclear terrorism. However, the process of implementing and reviewing deterrence-based strategies must be done at a pace matching the progression and spread of technological capabilities.

Given this, the Intelligence Community is the best candidate among federal agencies in the U.S. to support building effective cyber threat policy using deterrence for issues such as nuclear terrorism, as they possess the greater qualities of understanding the technological progression inherent to cyber threats as well as possess the greatest capacity at providing the necessary intelligence and guidance to existing agencies when dealing with the future of asymmetric threats. As literature regarding nuclear terrorism and cyberthreats continues to grow, there are many other questions guide further research. Understanding how strategists view asymmetric threats versus traditional inter-state conflict is important in developing sound national strategies that can guide the response to creating policy to address future threats. The establishment of norms for upcoming technologies is critical for curbing the growing threat and pacing at which cyberwarfare capabilities are developed and distributed. Determining the limitations of deterrence theory given a lack of rational actors, or indifferent threats, is necessary in future additions to third wave deterrence theory literature in order to better inform the limitations of deterrence theory. When addressing federal agencies, the question of how to promote and ensure inter-agency cooperation is important to the future success of national security issues as conflict and threats become more asymmetrical in nature. In promoting the further involvement of intelligence agencies, how can intelligence agencies be more effective in cooperating with other agencies? Can federal agencies

gather intelligence and operate effectively while not infringing on privacy and could these agencies be in a position to protect privacy without hampering security? Does the government have a responsibility to limit technological progression in the spirit of national security?

There is an abundance of research to be done as it relates to future applications of deterrence theory by policymakers for addressing nuclear security, cybersecurity, and terrorism. Overall, the findings of this paper address that the phases of deterrence theory applied to nuclear terrorism by policy-makers has shifted as a result of an increase in cyberthreats. In addition, the lack of cooperation among federal agencies to address cyberthreats can best be fulfilled by further integration and cooperation with intelligence agencies. Moving forward, it would be beneficial to review further documents as new technologies and threats emerge, necessitating new policy, and previously redacted information becomes declassified. As cyber threats and cyberwarfare capabilities continue to be developed and become more complex, yet available, it is paramount that nuclear security and policy be adaptable to these new and emerging threats. As non-state actors, such as terrorist organizations, continue to seek interest in the prospect of nuclear terrorism, U.S. national security policy must be able to adapt and be executed effectively as threats continue to emerge.

APPENDIX A: CODE SHEET

Date of Coding:
Name of Coder:
Sampling Information | ID#:

Document Title:

Agency/Branch:

Subcommittee:

Date:

Asset/System of Concern:

Non-State Actor Addressed:
Yes/No
(Name of non-state actors, terrorist, group, etc.)

Cyber Threats Addressed:
Yes/No
If Yes, **# of Times mentioned**
Phishing _____
Advanced Persistent Threat (APT) _____
Malware _____
Web Attacks_____
Denial of Service (DoS)_____
DDoS (DDoS)_____
Eavesdropping _____
Man in the Middle (MitM) _____
Insider _____
Artificial Intelligence (AI) _____
Quantum _____
Non-Specific (Name if provided)_____
Quotes
(Quote of Threat Addressed)

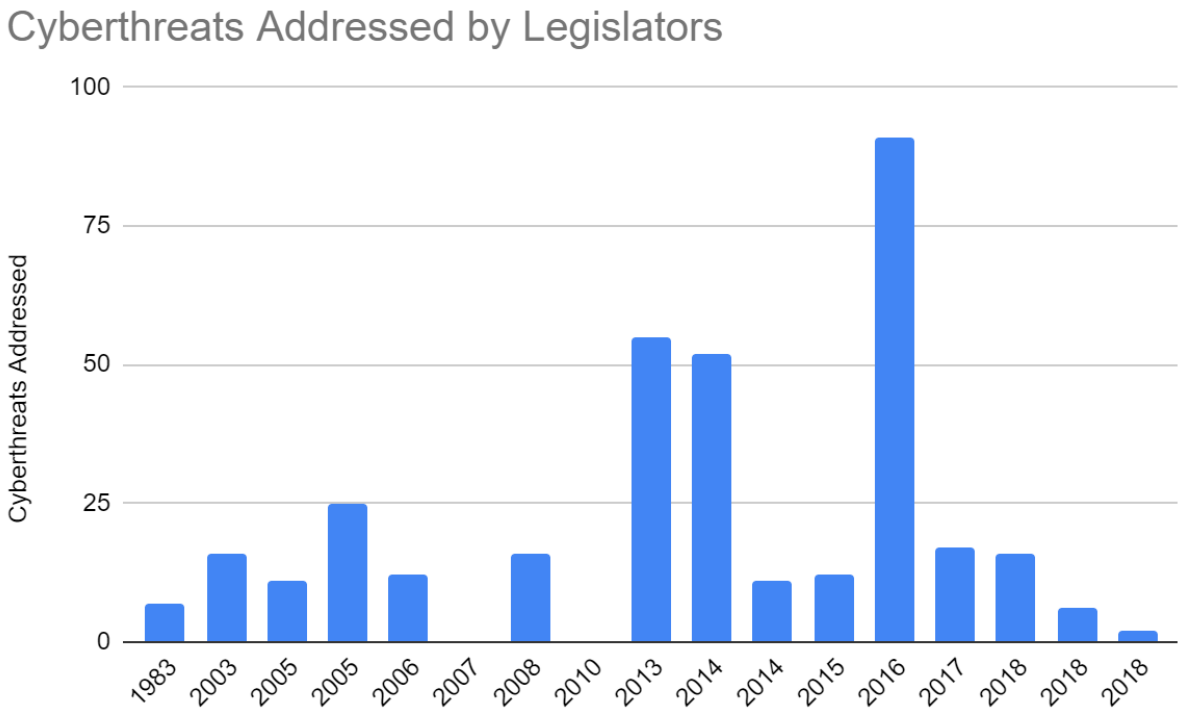
Future Threats Addressed?
Yes/No

Enforcement Guidelines
Yes/No

Reference to Past Policy
Yes/No
Positive/ Negative

Phase of Deterrence Theory
1/2/3/4 Type of Deterrence:_____ Target of Deterrence:_____

Figure A



Number of Times Cyber Threats were mentioned by legislators per document by month/year.

Figure B

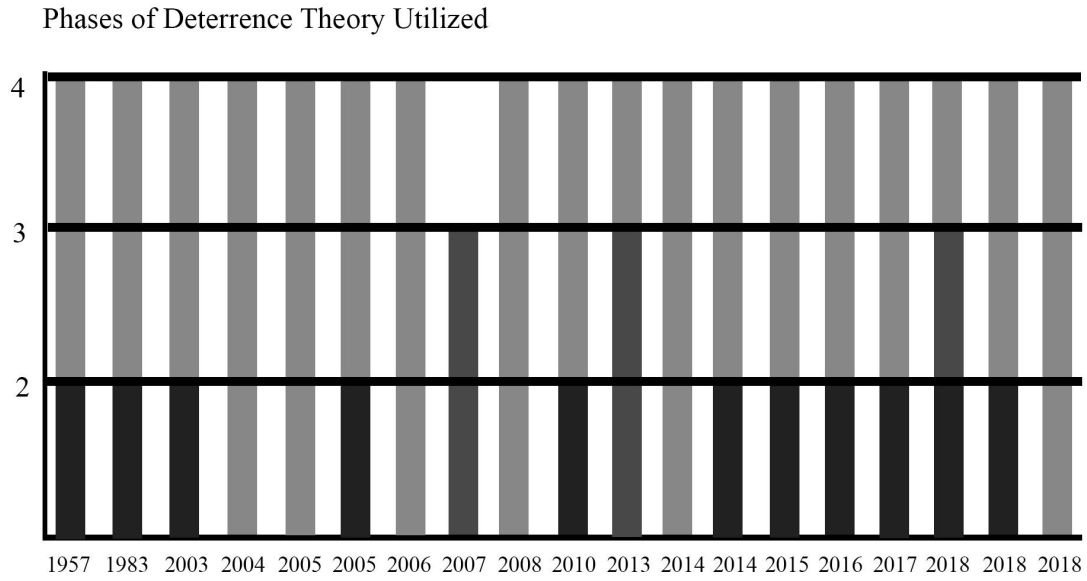


Figure C

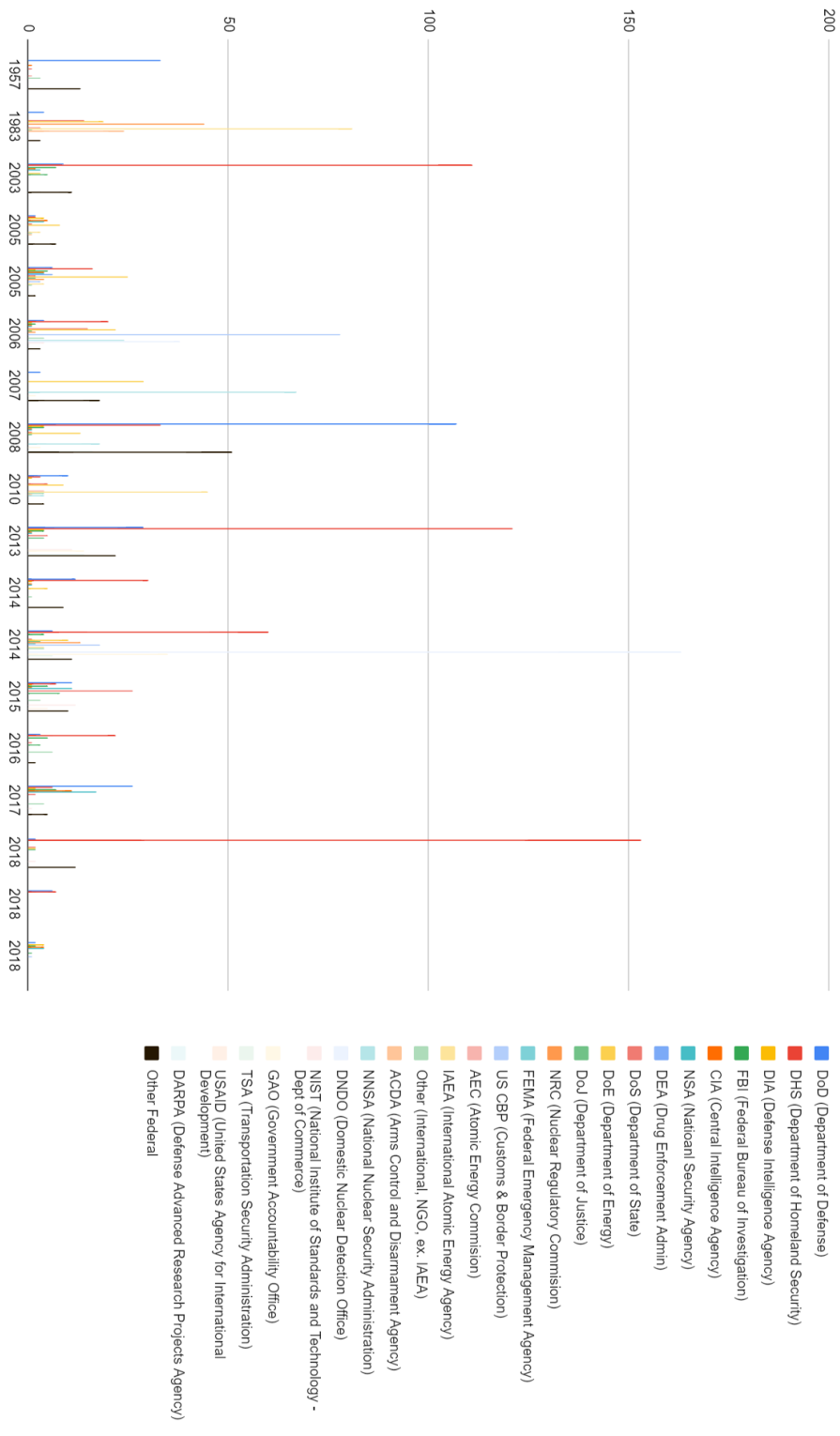
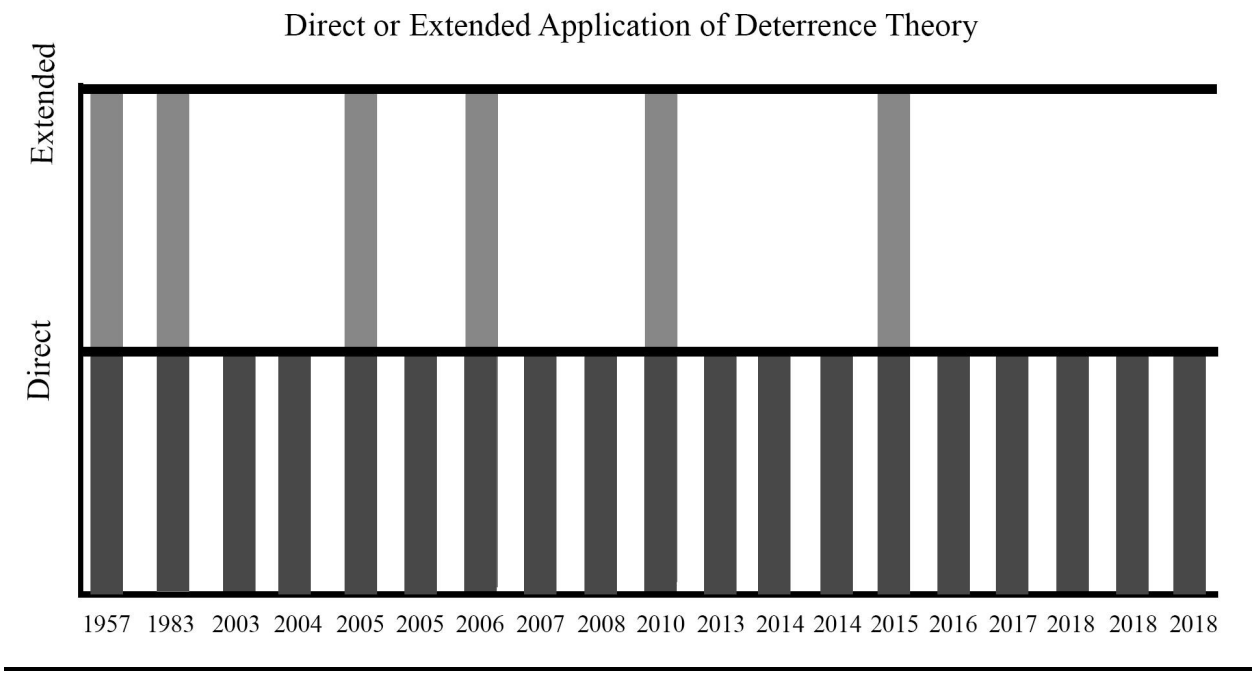

0
50
100
150
200
1957
1983
2003
2005
2005
2006
2007
2008
2010
2013
2014
2014
2015
2016
2017
2018
2018
2018
DoD (Department of Defense)
DHS (Department of Homeland Security)
DIA (Defense Intelligence Agency)
FBI (Federal Bureau of Investigation)
CIA (Central Intelligence Agency)
NSA (Natioanl Security Agency)
DEA (Drug Enforcement Admin)
DoS (Department of State)
DoE (Department of Energy)
DoJ (Department of Justice)
NRC (Nuclear Regulatory Commision)
FEMA (Federal Emergency Management Agency)
US CBP (Customs & Border Protection)
AEC (Atomic Energy Commision)
IAEA (International Atomic Energy Agency)
Other (International, NGO, ex. IAEA)
ACDA (Arms Control and Disarmament Agency)
NNSA (National Nuclear Security Administration)
DNDO (Domestic Nuclear Detection Office)
NIST (National Institute of Standards and Technology - Dept of Commerce)
GAO (Government Accountability Office)
TSA (Transportation Security Administration)
USAID (United States Agency for International Development)
DARPA (Defense Advanced Research Projects Agency)
Other Federal

Figure D


Direct or Extended Application of Deterrence Theory
Extended
Direct
1957 1983 2003 2004 2005 2005 2006 2007 2008 2010 2013 2014 2014 2015 2016 2017 2018 2018 2018

Bibliography

Allison, Graham T. *Nuclear Terrorism: The Ultimate Preventable Catastrophe*. New York: Henry Holt, 2004.

Auerswald, David. "Deterring Nonstate WMD Attacks." *Political Science Quarterly*, vol. 121, no. 4, 2006, pp.543-568.

Barnaby, Frank. *How to Build a Nuclear Bomb: and Other Weapons of Mass Destruction*. New York: Nation Books, 2004.

Bell, Mark S. "Defending the 'Acquisition-Use Presumption' in Assessing the Likelihood of Nuclear Terrorism." *International Studies Quarterly*, vol. 63, no. 3, Sept. 2019, pp. 774–778. *EBSCOhost*, doi:10.1093/isq/sqz004.

Bendiek, Annegret, and Tobias Metzger. "Deterrence Theory in the Cyber-Century." *Informatik*, 2015, pp. 553–570.

Berejikian, Jeffrey. "A Cognitive Theory of Deterrence." *Journal of Peace Research*, vol. 39, no. 2, 2002, pp. 141-167.

Beyza, Unal, and Patricia Lewis. "Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences." *Chatham House, The Royal Institute of International Affairs*, Jan. 2018, https://www.chathamhouse.org/sites/default/files/publications/research /2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

Biro, Lucian, et al. "Nuclear and Radiologic Terrorism Impact on National Security." *Romanian Journal of Forensic Science*, vol. 18, no. 5, Oct. 2017, pp. 2687–2693. *EBSCOhost*,search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=132542405&sit e=eds-live&scope=site.

Bowen, Wyn Q, et al. "Multilateral Cooperation and the Prevention of Nuclear Terrorism: Pragmatism over Idealism." *International Affairs*, vol. 88, no. 2, 20 Mar. 2012, pp. 349–368., doi:https://doi.org/10.1111/j.1468-2346.2012.01075.x.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. Oxford: Oxford University Press, 2009.

Brodie, Bernard, 1910-1978, editor. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Company, 1946.

Bunn, Matthew. President and Fellows of Harvard. *Securing the Bomb 2010: Securing All Nuclear Materials in Four Years.* Washington D.C.: Nuclear Threat Initiative, April 12, 2010. Retrieved 28 January 2013.

Bunn, Matthew. *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* Belfer Center for Science and International Affairs, Harvard Kennedy School, Mar. 2016,www.belfercenter.org/sites/default/files/legacy/files/Preventing NuclearTerrorism-Web.pdf.

Colbourn, Susan E. "No Use: Nuclear Weapons and U.S. National Security Policy by Thomas M. Nichols." *International Journal*, vol. 70, no. 2, 2015, p. 361-363. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edshol&AN =edshol.hein.journals.intj70.44&site=eds-live&scope=site.

Crenshaw, Martha, et al. "Coercive Diplomacy and the Response to Terrorism." *The United States and Coercive Diplomacy*, 2003. Washington D.C.: United States Institute of Peace Press, 2003.

Crenshaw, Martha, and Gary Lafree. *Countering Terrorism*. Washington D.C.: Brookings Institution Press, 2017.

Davis, Paul., Brian Michael Jenkins, *Deterrence and Influence in Counter-terrorism: A Component in the War on al Qaeda.* Santa Monica, CA: RAND, 2002.

Dogrul, Murat, et al. "Developing an international cooperation on cyber defense and deterrence against Cyber terrorism," *2011 3rd International Conference on Cyber Conflict*, IEEE, 2011, pp. 1-15.

Dunn, Lewis. *Influencing Terrorists' Acquisition and Use of Weapons of Mass Destruction*. Rome, Italy: NATO Defense College Presentation, Aug 5, 2008.

Dye, Robert Craig. *Update on the Status of Modernizing NC3*. New Mexico: Los Alamos National Laboratory, 2019.

Early, Bryan R., et al. "Should Conventional Terrorist Bombings Be Considered Weapons of Mass Destruction Terrorism?" *Dynamics of Asymmetric Conflict*, vol. 10, no. 1, Mar.2017, pp. 54–73. *EBSCOhost*, doi:10.1080/17467586.2017.1349327.

Eaves, Elisabeth. "What Does 'Nuclear Terrorism' Really Mean?" *Bulletin of the Atomic Scientists*, 17 Sept. 2018, thebulletin.org/2016/04/what-does-nuclear-terrorism-really-mean

Edelman, R. David. *Speakers: Cybersecurity at Executive Forum 2019*. Washington D.C.: Swedish-American Chambers of Commerce, June 13, 2019.

Feiveson, Harold A., et al. *Unmaking the Bomb: A Fissile Material Approach to Nuclear Disarmament and Nonproliferation*. Cambridge: The MIT Press, 2016.

Flynn, Stephen. *America The Vulnerable: How Our Government Is Failing to Protect Us from Terrorism*. New York: Harper Perennial, 2004.

Futter, Andrew. “Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy.” *Royal United Services Institute for Defense and Security Studies*, July 2016, pp. 1–48.

Futter, Andrew, and Des Browne. *Hacking the Bomb: Cyber Threats and Nuclear Weapons.* Washington D.C.: Georgetown University Press, 2018.

Gale, Robert P., and James O. Armitage. “Are We Prepared for Nuclear Terrorism?” *New England Journal of Medicine*, vol. 378, no. 13, 2018, pp. 1246–1254., doi:10.1056/nejmsr1714289.

Gallagher, Mark A., and Michael C. Horta. “Cyber Joint Munitions Effectiveness Manual (JMEM).” *American Intelligence Journal*, vol. 31, no. 1, Jan. 2013, pp. 73–81. *EBSCOhost*,search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=117031978&site=eds-live&scope=site.

Geers, Kenneth. “The Cyber Threat to National Critical Infrastructures: Beyond Theory.” *Information Security Journal: A Global Perspective*, vol. 18, no. 1, 3 Feb. 2009, pp. 1–7., doi:https://doi.org/10.1080/19393550802676097.

Geers, Kenneth. “The Challenge of Cyber Attack Deterrence.” *Computer Law & Security Review*, vol. 26, no. 2, 29 May 2010, pp. 298–303., doi:https://doi.org/10.1016/j.clsr.2010.03.003.

Geist, Edward. “Deterrence Stability in the Cyber Age.” *Strategic Studies Quarterly*, vol. 9, no.4, Winter 2015, pp. 44–61. *EBSCOhost*,search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=111210766&site=eds-live&scope=site.

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

Gerlini, Matteo, and Abdelwahed Chetaine. *Non-Proliferation, Safety and Nuclear Security: Collected Essays on Technologies and International Policies*. IOS Press, 2016. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1213910&site=eds-live&scope=site.

Graff, Garrett M. *Raven Rock: The Story of the U.S. Government's Secret Plan to Save Itself - While the Rest of Us Die*. New York: Simon and Schuster, 2017.

Grogan, Steven. “China, Nuclear Security and Terrorism: Implications for the United States.” *Orbis*, vol. 53, no. 4, Sept. 2009, pp. 685–704. *EBSCOhost*, doi:10.1016/j.orbis.2009.07.011.

Harknett, Richard. “The Logic of Conventional Deterrence and the End of the Cold War.” *Security Studies*, vol. 4, no. 1, 1994, p. 86-114.

Harknett, Richard J., et al. “Leaving Deterrence Behind: War-Fighting and National Cybersecurity.” *Journal of Homeland Security & Emergency Management*, vol. 7, no. 1, Jan. 2010, p. 1-22. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edb&AN=48990861 &site=eds-live&scope=site.

Harvey, Frank. “Rigor Mortis or Rigor, More Test: Necessity, Sufficiency, and Deterrence.” *International Studies Quarterly*, vol. 42, no. 4, 1998, pp. 3-37.

Heitzenrater, Chad, et al. “When the Winning Move Is Not to Play: Games of Deterrence in Cyber Security.” *Lecture Notes in Computer Science Decision and Game Theory for Security*, 2015, pp. 250–269., doi:10.1007/978-3-319-25594-1_14.

Hitch, Chalres J, and Roland N McKean. *The Economics of Defense in the Nuclear Age*. The RAND Corporation, 1960, https://www.rand.org/content/dam/rand/pubs/reports/2005/R346.pdf.

Hogan, David E, and Ted Kellison. “Nuclear Terrorism.” *The American Journal of Medical Sciences*, vol. 323, no. 6, June 2002, pp. 341–349., doi:https://doi.org/10.1097/00000441-200206000-00006.

Holloway, David. *Stalin and the Bomb*. CT: Yale, 1994.

Holsti, Ole R. *Content Analysis for the Social Sciences and Humanities*. Reading, MA: Addison-Wesley Pub., 1969.

Huth, Paul., Bruce Russett, “Testing Deterrence Theory: Rigor Makes a Difference” *World Politics* vol. 42, no. 4, 1990, pp.466-501.

Huth, Paul, and Bruce Russett. “What Makes Deterrence Theory Work? Cases from 1900 to 1980.” World Politics, vol. 36, no. 4, 1984, pp. 496-526.

Iasiello, Emilio. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security*, vol. 7, no. 1, Spring 2014, pp. 52–67. *EBSCOhost*, doi:10.5038/1944-0472.7.1.5.

Iqbal, Imrana. “International Law of Nuclear Weapons Nonproliferation: Application to Non-State Actors.” *Pace International Law Review*, vol. 31, no. 1, Winter 2018, pp. 1– 58. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=asn&AN=136003879 &site=eds-live&scope=site.

Jackson, Richard. *Writing the War on Terror: Language, Politics and Counter-terrorism.* Manchester: Manchester University Press, 2005.

Jackson, Richard., Jarvis, L., Gunning, J., & Breen-Smyth, M. *Terrorism: A Critical Introduction.* London, UK: Palgrave Macmillian, 2011.

Jajodia, Sushil, et al. *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Berlin, Germany: Springer, 2014.

Jervis, Robert, et al. *Psychology and Deterrence*. MA: John Hopkins University Press, 1985.

Jervis, Robert L. "The Confrontation Between Iraq and the Us: Implications for the Theory and Practice of Deterrence." *European Journal of International Relations*, vol. 9, no. 2, 2003, p. 315-337.

Joyner, Christopher C. "Countering Nuclear Terrorism: A Conventional Response." *International Affairs*, vol. 18, no. 2, 1 Apr. 2007, p. 225–251. doi:https://doi.org/10.1093/ejil/chm014.

Kaufmann, William W., "The Requirements of Deterrence"1945 November 15. Henry A. Kissinger Papers, Part II (MS 1981). Manuscripts and Archives, Yale University Library. 1956. http://hdl.handle.net/10079/digcoll/560733.

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

Klein, John J. "Deterring and Dissuading Nuclear Terrorism." *Journal of Strategic Security*, vol. 5, no. 1, 2012, pp. 15–30. *JSTOR*, www.jstor.org/stable/26463985.

Knopf, Jeffrey W. "Wrestling with Deterrence: Bush Administration Strategy After 9/11." *Contemporary Security Policy*, vol. 29, no. 2, 2008, pp. 229-26.

Knopf, Jeffrey W. "The Fourth Wave in Deterrence Research." *Contemporary Security Policy*, vol. 31, no. 1, 2010, pp. 1–33., doi:10.1080/13523261003640819.

Kramer, Franklin D, and Melanie J Teplinsky. "Cybersecurity and Tailored Deterrence." *Atlantic Council: Brent Scowcroft Center On International Security*, Dec. 2013, pp. 1–10.

Krippendorff, Klaus. *Content Analysis: An Introduction to its Methodology*. 4th Edition, New York:Sage Publications, 2018.

Kuperman, Alan J. *Nuclear Terrorism and Global Security: The Challenge of Phasing out Highly Enriched Uranium*. Routledge, 2014.

Kshetri, Nir. "Recent US Cybersecurity Policy Initiatives: Challenges and Implications." *Computer*, vol. 48, no. 7, 20 July 2015, pp. 64–69., doi:10.1109/MC.2015.188.

Lebovic, James. *Deterring International Terrorism and Rogue States: US National Security Policy After 9/11*. London, UK: Routledge, 2007.

Lebow, Richard Ned. *Between Peace and War: The Nature of International Crisis*. MA: John Hopkins University Press, 1981.

Lebow, Richard Ned, and Janice Gross Stein. "Rational Deterrence Theory: I Think, Therefore I Deter." *World Politics*, vol. 41, no. 2, 1989, pp. 208-224.

Lebow, Richard Ned, and Janice Gross Stein. "Deterrence: The Elusive Dependent Variable." *World Politics*, vol. 42, no. 3, 1990, pp. 336-369.

Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington D.C.: Center for Strategic and International Studies, Dec. 2002.

Libicki, Martin. *Cyberdeterrence and Cyberwar*. Washington D.C.: RAND, 2009.

Mayer, Klaus. "Security: Expand Nuclear Forensics." *Nature: International Weekly Journal of Science*, 27 Nov. 2013, pp. 461–462., doi:10.1038/503461a.

McIntosh, Christopher, and Ian Storey. "Response to Mark Bell's 'Defending the Acquisition- Use Presumption in Assessing the Likelihood of Nuclear Terrorism.'" *International Studies Quarterly*, vol. 63, no. 3, Sept. 2019, pp. 770–773. *EBSCOhost*, doi:10.1093/isq/sqz053.

McIntosh, Christopher, and Ian Storey. "Between Acquisition and Use: Assessing the Likelihood of Nuclear Terrorism." *International Studies Quarterly*, vol. 62, no. 2, June 2018, pp. 289–300. *EBSCOhost*, doi:10.1093/isq/sqx087.

Mearsheimer, John. *Conventional Deterrence*. Cornell University Press, 1983.

Morgan, Patrick M. *Deterrence: A Conceptual Analysis*. Beverly Hills: Sage Publications, 1983.

Morgan, Patrick M. *Deterrence Now.* Cambridge: Cambridge University Press, 2003.

Morgenstern, Oskar. *The Question of National Defense.* Xii, 306. New York: Random House, 1959.

Mowatt-Larssen, Rolf. "Nightmares of Nuclear Terrorism." *Bulletin of the Atomic Scientists*, vol.66, no. 2, 1 Mar. 2010, pp. 37–45., doi:https://doi.org/10.2968/066002005.

Murakami, Haruki, et al. *Underground*. New York: Vintage International, 2001.

Nacht, Michael. "The Future Unlike the Past: Nuclear Proliferation and American Security Policy." *International Organization*, vol. 35, no. 1, 1981, p.193-212. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edsjsr&AN=edsjsr.2706562&site=eds-live&scope=site.

Naseer, Rizwan, and Musarat Amin. "Nuclear Terrorism: Hype, Risks and Reality-A Case of Pakistan." *South Asian Studies (1026-678X)*, vol. 34, no. 2, July 2019, pp. 383–399. *EBSCOhost*,

search.ebscohost.com/login.aspx?direct=true&db=asn&AN=138601284&
site=eds-live&scope=site.

Newmeyer, Kevin P. "Who Should Lead U.S. Cybersecurity Efforts?" *PRISM*, vol. 3, no. 2, Mar. 2012, pp. 115–126.

Nye, Joseph S. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly*, vol. 2011, no. Winter, Jan. 2011, pp. 19-38. https://apps.dtic.mil/dtic/tr/fulltext/u2/a553620.pdf.

Nye, Joseph S. "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" *Bulletin of the Atomic Scientists*, vol. 69, no. 5, 1 Sept. 2013, pp. 8–14., doi:https://doi.org/10.1177/0096340213501338.

Osawa, Jun "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, 2017, pp. 113-131, DOI: 10.1080/13439006.2017.1406703

Oti, Enrique A. "Deterrence Has to Be Lethal." *Hoover Digest: Research & Opinion on Public Policy*, no. 4, Fall 2015, pp. 60–64. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=asn&AN= 110362995&site=eds-live&scope=site.

Pandza, Jasper. "Managing the Consequences of Nuclear Terrorism." *Survival: Global Politics & Strategy,* vol. 53, no. 5, 29 Sept. 2011, pp. 129–142., doi:https://doi.org/10.1080/00396338.2011.621637.

Richelson, Jefferey. "Defusing Nuclear Terror." *Bulletin of the Atomic Scientists*, vol. 58, no. 2, 1 Mar. 2002, pp. 38–43., doi:https://doi.org/10.2968/058002013.

Roesener, August G, et al. "Policy for US Cybersecurity." *Air and Space Power Journal*, vol. 2014, no. November-December, Dec. 2014, p. 38-54. https://apps.dtic.mil/dtic/tr/fulltext/u2/a617837.pdf.

Russett, Bruce. "The Calculus of Deterrence." *Journal of Conflict Resolution*, vol. 7, no. 2, 1963, pp. 97-109.

Salmon, Trevor. "Rationality and Politics: The Case of Strategic Theory." *British Journal of International Studies*, vol. 2, no. 3, 1976, pp. 293-310.

Schelling, Thomas C. *Arms and Influence.* Yale University Press, 1966. JSTOR, www.jstor.org/stable/j.ctt5vm52s. Accessed 8 Feb. 2020

Skylar, Vladimir. "Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities." *Information & Security: An International Journal*, vol. 28, no. 1, 1 Nov. 2012, pp. 98–107., http://defencemanagement.org/system/files/28.08_Sklyar.pdf.

Smith, Derek. *Deterring America: Rogue States and the Proliferation of Weapons of Mass Destruction.* Cambridge: Cambridge University Press, 2006.

Snyder, Glenn. *Deterrence and Defense: Toward a Theory of National Security*. Princeton: Princeton University Press, 1961.

Snyder, Glenn, and Paul Diesing. *Conflict Among Nations.* Princeton: Princeton University Press, 1977.

Solms, Rossouw von, and Johan van Niekerk. "From information security to cyber security." Computers & Security, vol 38, 2013, pp. 97-102.

Steinbruner, John. "Beyond Rational Deterrence: The Struggle for New Conceptions." *World Politics*, vol. 28, no. 2, 1976, pp. 223-245.

Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy*, 33:1, 2012. pp. 148-170, DOI: 10.1080/13523260.2012.659597

Taddeo, Mariarosaria. "The Limits of Deterrence Theory in Cyberspace." *Philosophy & Technology*, vol. 31, no. 3, Sept. 2018, pp. 339–355.

Tomes, Robert R. "Socio-Cultural Intelligence and National Security." *Parameters: U.S. Army War College*, vol. 45, no. 2, Summer 2015, pp. 61–76. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=132942134 &site=eds-live&scope=site.

Trautman, Lawrence J. "Cybersecurity: What About U.S. Policy?" *SSRN Electronic Journal*, 2015, doi:10.2139/ssrn.2548561, pp. 1-51.

United States Government Accountability Office. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, Report to Congressional Addressees, February 2013.* Washington D.C.: Government Accountability Office, 2013.

United States House of Representatives. *Building a Nuclear Bomb: Identifying Early Indicators of Terrorist Activities: Hearing Before the Subcommittee on Prevention of Nuclear and Biological Attack of the Committee on Homeland Security, One Hundred Ninth Congress, May 26, 2005.* Washington D.C.: U.S. Government Printing Office, 2005.

United States House of Representatives. *Trends in Illicit Movement of Nuclear Materials: Hearing Before the Subcommittee on Prevention of Nuclear and Biological Attack of the Committee on Homeland Security, One Hundred Ninth Congress, First Session, September 22, 2005.* Washington D.C.: U.S. Government Printing Office, 2007.

United States House of Representatives. *Enlisting Foreign Cooperation in U.S. Efforts to Prevent Nuclear Smuggling: Hearing Before the Subcommittee on Prevention of Nuclear and Biological Attack of the Committee on Homeland Security, One Hundred Ninth Congress, Second Session, May 25, 2006.* Washington D.C.: U.S. Government Publishing Office, 2007.

United States House of Representatives. *The Department of Energy's Implementation of the National Nuclear Security Administration Act of 2000: Hearing before the Strategic Forces Subcommittee of the Committee on Armed Services, One Hundred Tenth Congress, First Session, January 31, 2007.* Washington D.C.: U.S. Government Publishing Office, 2007.

United States House of Representatives. *Stopping the Spread of Nuclear Weapons, Countering Nuclear Terrorism: The NPT Review Conference and the Nuclear Security Summit: Hearing Before the Committee on Foreign Affairs, One Hundred Eleventh Congress, Second Session, April 21, 2010.* Washington D.C.: U.S. Government Printing Office, 2010.

United States House of Representatives. *Protecting the Homeland from Nuclear and Radiological Threats: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives, One Hundred Thirteenth Congress, Second Session, July 29, 2014*. Washington D.C.: U.S. Government Publishing Office, 2015.

United States House of Representatives. *Electromagnetic Pulse (EMP): Threat to Critical Infrastructure: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives, One Hundred Thirteenth Congress, Second Session, May 8, 2014*. Washington D.C.: U.S. Government Printing Office, 2015.

United States House of representatives. *Cybersecurity: Setting the Rules for Responsible Global Cyber Behavior: Hearing before the Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy of the Committee on Foreign Relations, United States Senate, One Hundred Fourteenth Congress, First Session, May 14, 2015*. Washington D.C.: U.S. Government Publishing Office, 2015.

United States House of Representatives. *Emerging Cyber Threats to the United States: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives, One Hundred Fourteenth Congress, Second Session, February 25, 2016*. Washington D.C.: U.S. Government Publishing Office, 2016.

United States House of Representatives. *CDM, the Future of Federal Cybersecurity: Hearing before the Subcommittee on Cybersecurity and Infrastructure Protection*

of the Committee on Homeland Security, House of Representatives, One Hundred Fifteenth Congress, Second Session, January 17, 2018. Washington D.C.: U.S. Government Publishing Office, 2018.

United States President's Science Advisory Committee, Security Resources Panel. *Deterrence and survival in the nuclear age (the "Gaither report" of 1957)* MI: University of Michigan, 1957.

United States Senate. *Nuclear Non-Proliferation Act: Joint hearing before the Committee on Foreign Relations and the Subcommittee on Energy, Nuclear Proliferation, and Government Processes of the Committee on Governmental Affairs, United States Senate, Ninety-eighth Congress, first session.* Washington D.C.: U.S. G.P.O., September 30, 1983.

United States Senate. *Technologies to Combat Weapons of Mass Destruction: Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, United States Senate, One Hundred Tenth Congress, Second Session, March 12, 2008*. Washington D.C.: U.S. G.P.O., 2008.

United States Senate. *Foreign Cyber Threats to the United States: Hearing Before the Committee on Armed Services, One Hundred Fifteenth Congress, First Session, January 5, 2017.* Washington D.C.: U.S. Government Publishing Office, 2019.

United States, The White House. *The National Strategy to Secure Cyberspace.* Washington D.C.: The White House, 2003.

United States, The White House. *National Cyber Strategy of the United States of America*. Washington D.C.: The White House, 2018.

United States, The White House. *National Strategy for Countering Weapons of Mass Destruction Terrorism.* Washington D.C.: The White House, 2018.

Van der Meer, Sico. *Cyber Warfare and Nuclear Weapons: Game-changing Consequences?* Netherlands: Netherlands Institute of International Relations, December (2016).

Volders, Brecht. "Nuclear Terrorism: What Can We Learn from Los Alamos?" *Terrorism & Political Violence*, vol. 31, no. 5, Sept. 2019, pp. 1006–1025. *EBSCOhost*, doi:10.1080/09546553.2017.1304383.

Volders, Brecht, and Tom Sauer. *Nuclear Terrorism: Countering the Threat*. London, U.K.: Routledge, 2017.

Walt, Stephen. "Rigor or Rigor Mortis, Rational Choice and Security Studies." *International Security*, vol. 23, no. 4, 1999, pp. 5-48.

Wenger, Andreas, and Alex Wilner. *Deterring Terrorism: Theory and Practice*. Stanford Security Studies, an Imprint of Stanford University Press, 2012.

Weiss, Michael, and Hassan Hassan. *ISIS: Inside the Army of Terror*. New York: Regan Arts, 2016.

Wilner, Alex. “Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism” *Journal of Strategic Studies* vol. 34, no. 1, 2011, pp. 3-37.

Wyn, Bowen. “Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism” *Contemporary Security Policy* vol. 25: no. 1, 2004, pp. 54-70.

Zulaika, Joseba and William Douglass. "Drones, Witches and other Flying Objects: The Force of Fantasy in US Counterterrorism". *Critical Studies on Terrorism* 2012, pp. 51-68.