Spring 3-2023

All Bark and No Byte: A Case Study on Nuclear Weapons' Role in Cyber Deterrence

Phuc Nguyen
University of Nebraska - Lincoln

ALL BARK AND NO BYTE:
A CASE STUDY ON NUCLEAR WEAPONS' ROLE IN CYBER DETERRENCE

An Undergraduate Honors Thesis
Submitted in Partial fulfillment of
University Honors Program Requirements
University of Nebraska-Lincoln

By
Phuc D. Nguyen, BA
Political Science
College of Arts and Sciences

March 13, 2023

Faculty Mentors:
Tyler White, PhD, Political Science
Geoff Lorenz, PhD, Political Science

Abstract

In what some scholars consider a marked departure from its traditional policy, the U.S.' 2018 Nuclear Deterrence Posture Review declared that the U.S. would consider the use of nuclear weapons in response to "significant, non-nuclear strategic attacks." However, despite real-world examples of the type of significant cyberattacks on U.S., allied, or partner civilian population or infrastructure alluded to in the Review, the factors that might trigger multidomain escalation remain underexplored, which creates a credibility gap in the U.S.' deterrence policy. This paper explores these factors by providing a case study of the North Korean WannaCry and Russian NotPetya cyberattacks and compares the potential flashpoints caused by each attack with declared U.S. nuclear policy. In so doing, it examines how the presence of a traditional nuclear deterrent affects a state's ability to deter cyberattacks.

Key Words: Nuclear policy, nuclear deterrence, cyber deterrence, WannaCry, NotPetya

Introduction

In February 2018, the Trump administration released the unclassified version of its Nuclear Posture Review (NPR), thus heralding what some scholars consider to be a significant departure from previous United States (U.S.) nuclear policy. Whereas the U.S.' nuclear policy under the Obama administration had come the closest it has ever been to a sole-purpose posture, the new 2018 NPR declared that the U.S. would also consider the use of nuclear weapons in response to "significant, non-nuclear strategic attacks," introducing the possibility that cyberattacks might be met by nuclear retaliation. Despite a number of significant cyberattacks having occurred both before and since the Trump NPR's publication, the literature on cyber deterrence remains both theoretical and lacking in case studies. Additionally, for all the criticism that the NPR's new stance received, few studies have given serious thought to how nuclear weapons and attacks might influence cyber deterrence, despite the fact that the reverse—cyberattacks' effect on nuclear deterrence—has been the subject of careful scrutiny (Gartzke and Lindsay 2017; Acton 2018).

My paper seeks to address this gap by determining how the threat of a traditional nuclear deterrent affects the U.S.' ability to deter against cyberattacks. Based on the research of Rid (2012) and Kreps and Schneider (2019), I argue that, even when attacks can be attributed to specific actors, threatening a nuclear response has little effect in deterring cyberattacks because such a policy suffers from a credibility problem: namely, cyberattacks, even ones as virulent as the ones under investigation, are usually only capable of inflicting impermanent and, ultimately, transient damage, making it difficult for them to reach the level of a strategic attack. Without passing this declaratory threshold, among others, the U.S. will likely struggle to justify the significant political costs that come with nuclear weapons use. As a result, it is unlikely that the threat of nuclear retaliation will be able to credibly deter cyberattacks unless said attacks succeed where NotPetya and WannaCry failed and affect their target states substantially and for long enough that it generates permanent and physical effects.

What follows is a case study of two of the widest-reaching and costliest cyberattacks to date, WannaCry and NotPetya, to determine the extent to which they match the qualifications for what cyberattacks merit a nuclear response per the Trump administration's declaratory policy, with the underlying assumption being the declaratory policy precedes the use of a nuclear weapon on the causal chain. In other words, if it fails to meet the NPR's conditions, then nuclear use is likely a non-option. To this end, I use open-source information collected from official publications and announcements from governments, international organizations, newspapers, cybersecurity organizations, and, where applicable, think tanks. The paper proceeds in four parts: first, I contextualize my research question in relation to the literature on cyber and cross-domain deterrence; second, I provide an analysis of the Trump administration's nuclear policy, focusing in particular on its NPR and how it compares to the Obama administration's NPR; and third, I summarize the events and effects of the WannaCry and NotPetya attacks before finally conducting an evaluation on the extent to which the effects of these attacks match key conditions outlined by U.S. declared policy.

This paper does not seek to argue why WannaCry and NotPetya failed to elicit a nuclear or conventional response; rather, it leverages the extraordinary scale and nature of these attacks to retroactively apply the Trump administration's NPR and establish a lower bound for so-called "significant" non-strategic threats. U.S. nuclear policy has always sought to satisfy two paradoxical desires: on the one hand, the U.S. seeks to maintain some strategic ambiguity to maximize its freedom of action; on the other, the traditional view of effective deterrence is it depends upon the clear delineation of what is considered bad behavior and what said behavior's consequences are. As these two cases demonstrate, however, cyber deterrence differs from deterrence in the physical domains. Moreover, NotPetya and WannaCry raise important questions about how willing and actually capable the U.S. is of following through on its nuclear threats in cyberspace. By making a threat which it will never be able to follow through on, the U.S. risks diminishing its overall credibility and the effectiveness of its other threats. Therein lies the value of this paper: by seeking to discern where U.S. nuclear posture falls short, this paper will help policymakers better determine how best to deter future cyberattacks and whether pursuing it through the threat of nuclear weapons is a worthwhile endeavor.

Literature Review

Much of the literature on cyber deterrence draws from that on nuclear deterrence. Thomas Schelling's observations that threats and the resolve to carry them out must be clearly communicated to would-be adversaries have long been of interest to security scholars. By noting that an adversary must both correctly interpret the redlines established by the deterring actor and believe that the actor is capable of realizing its declarations, Schelling underscored the importance of credibility to an effective deterrence (Schelling 1966). However, it was easy for Schelling to axiomatically assume that the attribution of an attack is possible due to the physically observable nature of attacks in the nuclear domain. Conversely, cyberattacks lack the physical element that attacks in the other traditional domains of war do. In addition, obfuscation methods abound, and the attribution process is so technically complex that there is often a large delay between the time of the incident and the identification of the perpetrators, which causes the weight of retaliatory threats to diminish (Brantly 2018). These factors have led some scholars to conclude that attacks in cyber are considerably more difficult to attribute (Betts 2002; Libicki 2009; Nye Jr 2011; Iasiello 2013). Without the ability to identify attackers and hold their interests at ransom, it is difficult to carry out counterattacks, let alone demonstrate a willingness to follow through on them, and thus, the effectiveness of deterrence by punishment suffers. Consequently, deterrence by denial has been the more widely-accepted strategy between the two in cyberspace.

Recent studies have taken a different stance *vis-a-vis* the attribution problem in cyber. The sophistication required to code malicious, large-scale, and genuinely disruptive attacks cannot have the benefit of assuming anonymity, as such technical sophistication creates opportunities for error in either the coding or the operation itself that may assist victims with attribution (Lindsay 2013). Some even go as far as to argue that the attribution problem and offensive domain paradigms in the cyber deterrence literature are of little importance because the strategic context and operational realities of attacking certain actors in cyberspace narrows down the list of potential attackers, and there is little empirical evidence to support the offensive paradigm (Tor 2017). In other words, despite the fact that deterrence by punishment may not be entirely meaningless in cyber, the challenges related to its implementation dampen its effectiveness therein (Iasiello 2013; Nye Jr 2017).

In addition to influencing each other's theoretical paradigms, the relationship between the cyber and nuclear domains has also drawn interest because of the escalatory risks associated with the cyber-nuclear nexus. That is, cyberattacks have the potential to erode the stability of nuclear deterrence, particularly through the U.S.' nuclear command, control, and communications (NC3) architecture, which connects the national command authority to nuclear forces and provides the means for U.S. officials to detect, respond to, and order their own attacks. As they are now, these systems are increasingly antiquated. Although the age of the NC3 architecture means that adversaries have less forms of remote access to exploit, it also decreases the systems' overall effectiveness. The U.S. has taken steps to modernize its NC3 architecture from the legacy systems it currently employs, but doing so comes at the cost of creating new access vectors for adversaries. Moreover, as the U.S. continues to update its systems, certain redundancies are being eliminated (e.g., reducing the number of satellites capable of transmitting nuclear employment orders). These changes decrease the overall resilience of NC3 systems to cyberattacks while simultaneously increasing their effectiveness and introducing new attack vectors (Gartzke and Lindsay 2017; Acton 2018). As a result, there is a concern that a cyberattack on NC3 systems will compromise the integrity of the U.S.' second-strike capabilities.

Although threat actors might generally be deterred from attacking NC3 assets, the increasingly dual-use nature of these assets makes it difficult for attackers to distinguish between nuclear and nonnuclear weapons, heightening the risk of an incidental attack. Thus, for example, pure cyber espionage may be indistinguishable to victims from a move to disable their NC3 capabilities (Acton 2018). In turn, this ambiguity increases a victim's uncertainty, contributes to crisis instability, and incentivizes them to pursue more escalatory deterrence measures and attempts at limiting damage to themselves in what Acton (2018) terms "misinterpreted warning" and "the damage-limitation window," respectively. Indeed, systems need not even be actively degraded: the very possibility of latent malware may make leaders wary of information from early-warning systems (Klare 2019). Further exacerbating this problem is the fact that the number of escalation mechanisms increases during crises, when leaders in time-sensitive, highstress environments are likelier to misperceive situations (Acton 2020). Put briefly, there is a robust literature on how the cyber domain affects nuclear deterrence.

The same cannot be said of the reverse. To be sure, think tanks have spared no amount of ink expressing their views on the topic; however, with regards to academic research, little has been said about how the nuclear domain could potentially affect cyber deterrence. What studies that do exist on related topics only address the nuclear-to-cyber pathway tangentially, if at all. For example, scholars might examine the implications of certain administrations' nuclear policies, but do little to connect them to the cyber domain (Hayes 2018). As a result, although it is now more evident than ever that cyberattacks must clear certain thresholds in order to merit violent physical responses in general (Rid 2012; Rid 2013; Borghard and Lonergan 2019; Schneider 2020), the extent to which these so-called escalation firebreaks affect the likelihood of a nuclear response to a cyberattack remains understudied, to say nothing of the credibility of making such a retaliatory threat. Of course, it does not help matters that, to date, there has yet to be a cyberattack which has elicited a conventional response, let alone a nuclear one.

Besides the previous explanation, another possible contributing factor to the above gap in the literature is the nuclear taboo. The nuclear taboo is a *de facto* Cold War-era norm that stigmatizes the use of any kind of nuclear weapons (Tannenwald 2005). Nuclear weapons are uniquely destructive, but because of that same highly destructive quality, they are largely a non-option except for use as a deterrent and as a means to induce strategic stability (Hayes 2018). In the public's and some U.S. officials' view, the use of these weapons, even smaller tactical ones, constitutes such a severe breach of morals and American values that their use is illegitimate, to the point where the political costs of deploying one apparently outweighed the loss of the Vietnam War (Tannenwald 1999, 2012; Pant 2012). Considering that the dominant American view of nuclear weapons is that they only exist to never be used (Hayes 2018), questions pertaining to genuine nuclear use may seem superfluous.

Yet, given the growing value of offensive measures to both U.S. officials and academics in preventing cyber threats, this is an area that merits research. Besides the attribution problem discussed earlier, the asymmetry of reliance and capability between technologically-advanced states, who are best-equipped to launch offensive cyberattacks, and less technologically-capable states and non-state actors also makes it difficult to credibly threaten tit-for-tat deterrence because a power imbalance exists, and actors less dependent on cyber platforms will be less impacted by their loss (Lupovici 2011; Wilner 2019). As a result, this has led to the view that cyber is “inherently” cross-domain (Lindsay and Gartzke 2022). That is, the most effective means of deterrence are those that threaten to punish assets in one domain to deter attacks in others (Borghard and Lonergan 2017; Lonsdale 2017; Schneider 2020), with some caveats owing to the variations in the definition of cross-domain deterrence: although the Defense Department (DoD) normally defines it across the five traditional domains of land, sea, sky, space, and cyber (Mallory 2018), others define it based on weapons and types of belligerents (Dawkins 2009; Scouras, Smyth, Edward, and Mahnken, Thomas 2014; Lindsay and Gartzke 2019).

Similar to the traditional conceptions of deterrence discussed prior, though, cross-domain deterrence also has its limitations. First, the bar for effective deterrence is high: the American public is generally reluctant to resort to escalatory measures against cyberattacks and is only willing to support retaliation against cyberattacks that target civilian infrastructure and NC3 assets (Kreps and Schneider 2019; Schneider 2020). In addition, some types of cyberattacks are more likely than others to escalate to the physical world. For example, subversion, defined as the “deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order" (e.g., via propaganda) is more likely to lead to violence than sabotage (Rid 2012; Rid 2013), as are those cyberattacks that can generate the violence and horror necessary to galvanize the public and officials (Borghard and Lonergan 2019). Moreover, crossing domains may inadvertently escalate a conflict. Victims attempting to retaliate against non-state actors may impinge on the perpetrators' host country's sovereignty in their pursuit (Sterner 2011), or, alternatively, mutual misperceptions resulting from an asymmetry of available information and incentives to misrepresent them may embolden adversaries and trigger inadvertent escalation (Liff 2012). Consequently, although cross-domain deterrence is gaining traction among academics and the U.S. national security enterprise as an option to circumvent some of the traditional challenges associated with the cyber domain, it should not be treated as a silver bullet.

The value of this paper is twofold. To date, most of the cyber deterrence literature has been theoretical, and case studies on the subject remain lacking (Goodman 2010; Soesanto and Smeets 2021). This gap has left scholarly opinions on the very efficacy of cyber deterrence divided, with little empirical data to support them. In addition, as already discussed, although much has been written on how cyberattacks erode nuclear deterrence, there is little in the way of research explicitly focused on the reverse, despite US policymakers' apparent interest in applying nuclear threats to achieve cyberdeterrence. This study aims to contribute to the literature first, by examining in detail the events and consequences of two major cyberattacks and, by extension, serving as another aggregate of sources and analyses for future scholarship on them. Second, in grounding its analysis in the context of nuclear responses to cyberattacks, it seeks to stimulate further discourse on the relationship between nuclear weapons and cyber deterrence. Specifically, it questions the wisdom of such a move, both in how possible it is to implement and whether it is the most effective deterrent option available. With a clearer understanding of the role(s) that nuclear weapons can play in deterring cyberattack, U.S. policymakers will be able to create more effective policies to protect the American people.

The Trump Administration's Nuclear Declaratory Policy

The Trump administration situated its NPR within the context of a "worsening" security environment (U.S. Department of Defense 2018). Although both the Obama and Trump NPRs noted that the world was changing or evolving, respectively, by 2018, the source and range of new threats had expanded significantly: Obama was chiefly concerned with the prevention of nuclear proliferation amongst states and terrorist groups; Trump, meanwhile, argued that "There now exists an unprecedented range and mix of threats, including major conventional, chemical, biological, nuclear, space, and cyber threats, and violent non-state actors" which produced "uncertainty and risk" (U.S. Department of Defense 2018). U.S. relations with China and Russia had worsened, nuclear-capable states like Russia and North Korea were placing greater emphasis on nuclear force, and all three countries were growing increasingly aggressive in outer space and cyberspace. With arms control measures and the conditions to establish them deteriorating, despite the U.S.' efforts to abide by them, it became necessary to reevaluate the U.S.' nuclear posture.

Under these circumstances, nuclear weapons took on a special value to the Trump administration. Eschewing a "one size fits all" deterrence approach in favor of a flexible and tailored force that could match the diversity of security challenges, the Trump NPR stated that without nuclear deterrence, U.S., allies, and partners "would be vulnerable to coercion and attack by adversaries who retain or expand nuclear arms and increasingly lethal capabilities." Nuclear capabilities stood apart as a "necessary, unique, and currently irreplaceable" maximizer of the U.S.' freedom of action and deterrence credibility (U.S. Department of Defense 2018). To those ends, the administration called for an expansion of the U.S.' nuclear options to include low-yield capabilities, a move criticized by some scholars for being a tacit admission by the DoD that limited strategic nuclear war was possible (Brown 2018)—and for reversing the conventional argument that lower-yield nuclear weapons lowered the nuclear threshold (Stevenson 2018). Thus, believing that the breadth of security challenges could only be matched by a corresponding breadth of nuclear options (Peczeli 2018), the Trump administration replaced nuclear stability with nuclear deterrence as the centerpiece of the U.S.' new nuclear policy.

In addition to expanding the variety of nuclear weapons at the U.S.' disposal, the Trump NPR also broadened the conditions under which they could be used. The Obama administration's NPR had declared that it "will work to establish the conditions" under which the "sole purpose" of nuclear weapons would be to deter other nuclear attacks against itself or its allies and partners, the closest it has ever approached a sole-purpose posture (Peczeli 2018). Hence, the argument that "the role of U.S. nuclear weapons to deter and respond to non-nuclear attacks—conventional, biological, or chemical—has declined significantly" (U.S. Department of Defense 2010). In contrast, the Trump administration's National Security Strategy (NSS) declared that nuclear deterrence was "essential to prevent nuclear attack, non-nuclear strategic attacks, and large-scale conventional aggression." Therefore, the U.S. would entertain employing nuclear weapons

> in extreme circumstances to defend the vital interests of the United States, its allies, and its partners. Extreme circumstances could include significant non-nuclear strategic attacks. Significant non-nuclear strategic attacks include, but are not limited to, attacks on

> the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities (U.S. Department of Defense 2018).

In so doing, the Trump NPR reversed its predecessor's near-sole-purpose posture to once again potentially include a nuclear response to a non-nuclear one, revised the definition of non-nuclear attacks to now include cyberattacks, and brought civilian populations and infrastructure under the U.S.' explicit protection where they had previously lacked such focus. Notably, this was not the first policy document where the Trump administration tried to establish the link between cyberattacks and the threat they pose: the NSS, which was released two months prior, claimed that the spread of inexpensive weapons and cyber tools made it possible for adversaries to conduct non-nuclear strategic attacks "in ways that could cripple our economy and our ability to deploy our military forces." Reservations about the policy wisdom behind such a move notwithstanding, these changes gave credence to the view that the Trump NPR had an "elastic view" of the extreme circumstances meriting a nuclear response (Brown 2018), especially compared to its predecessor.

Several terms in the NPR's declaration clearly act as qualifiers to a U.S. nuclear response. Together, they stipulate the apparent nature of an attack, what it must threaten, and the target thereof; however, despite their importance, they are ill-defined within the document itself. For example, the concept of a strategic attack does not appear in the Obama administration's NPR nor does it feature in either NSS released by it; its use in the NPR is specific to the Trump administration. The term borrows from the Air Force doctrine of the same name for offensive actions targeting an adversary's centers of gravity in order to destroy their freedom of action, physical strength, or will to fight (Carlino 2002). Put briefly, then, strategic attacks are not distinguished by the weapons used to carry them out, but by how they catastrophically influence an adversary's ability and will to recover equilibrium and, ultimately, wage war (Thieret et al. 1996).

Likewise nebulous within the NPR are what constitutes America's vital interests and to which allies and partners its nuclear umbrella applies, though again, outside sources provide clues. The Trump NSS outlines four pillars considered vital national interests for the U.S.: first, the protection of the homeland, the American people, and the American way of life; second, the promotion of American prosperity; third, the preservation of peace through strength; and finally, the advancement of American influence. Expanding on the first pillar, the Trump administration also promises it "will protect our critical infrastructure and go after malicious cyber actors." Later, though it does not provide a detailed list of U.S. allies and partners, the Trump NSS notes that its nuclear deterrent extends to "more than 30 allies and partners"—presumably, the then-28 other members of the North Atlantic Treaty Organization (NATO), who are commonly recognized as official U.S. allies (Lange 2018); and South Korea, Japan, and Australia, all of whom are also allies through treaty-based pledges (Spector 2022). It is less clear to which partners the Trump administration refers to in both the NPR and NSS, a situation made all the more difficult by the DoD's lackluster definition that partnerships are those less-formal relationships that "usually focus on something mutually beneficial during a specific amount of time or for specific circumstances" (Lange 2018). However, this difficulty may well be a case of strategic ambiguity to preserve the U.S.' freedom of action in the face of so many qualifiers to a nuclear response. Nevertheless, the underlying implication is clear: the U.S. would only consider the use of nuclear weapons in response to attacks that target the U.S., NATO members, South Korea, Japan, Australia, and an unspecified list of partners; threaten one of the four vital national interests outlined by the NSS, and catastrophically affect their victims' will and war-waging ability.

WannaCry and NotPetya: Who, What, When, Where, How

The history of both WannaCry (or WannaCryptor) and NotPetya began on March 14, 2017, when Microsoft released a patch for a zero-day security vulnerability by the name of EternalBlue, which allowed attackers to remotely run any code on a victim's device. Though this patch preceded both attacks by as much as two months, businesses and organizations were slow to update their devices for any number of budgetary, bureaucratic, or perceptual reasons (MacKenzie 2019). The following month, a group by the name of the Shadow Brokers leaked EternalBlue to the public alongside other tools allegedly belonging to the National Security Agency (Greenberg 2018), providing hackers with a novel infection vector and enabling them to combine it with other malware to destructive effect.

On May 12, 2017, WannaCry, a ransomware worm developed by the North Korea-backed Lazarus Group (U.S. Department of Justice 2018a), became the first major cyberattack involving the EternalBlue exploit. Ransomware is malware that denies users access to their files, systems, or networks, while a computer worm is a self-replicating malware that spreads to other computers. WannaCry combined EternalBlue, which allowed it to remotely access vulnerable devices, much as with NotPetya, with a backdoor implanting malware named DoublePulsar to install itself on devices and encrypt them (McNeil 2017). Ransom notes initially demanded $300 from the victims in exchange for decrypting files, with a failure to pay resulting in the extortion price doubling after 3 days. WannaCry's general classification as ransomware suggests criminal or profit-driven intent. However, an affidavit released by the Justice Department indicates that

WannaCry was unusual for ransomware in that payment did not guarantee decryption, even a year later, and it self-propagated but did not appear to be targeting any persons or groups in particular (U.S. Department of Justice 2018b). Information on WannaCry's patient zero varies: global heat maps of attacks detected by Malwarebytes' cybersecurity software suggest the first computers were infected in Cheboksary, Russia and Zhytomyr, Ukraine (WannaCry Ransomware Infection Heat Map 2017), while a report from another cybersecurity company claims it began somewhere in southeast Asia, specifically, Hong Kong, India, or the Philippines (Brenner 2017).

In total, over 200,000 computers across 150 countries and a variety of sectors (e.g., healthcare, logistics, telecommunications, automotive, etc) were affected (Shea 2017; What was WannaCry? n.d.). Of WannaCry's victims, India, Taiwan, and Ukraine were among three of the most affected (Jones and Bradshaw 2017), though the British healthcare system remains one of the most well-known. In 2017, there were roughly 235 trusts, public entities roughly comparable to a corporation, operating under the British National Health Service. When WannaCry struck, over 60 of those trusts were affected—or about 20% of the United Kingdom's total public healthcare system (NHS cyber-attack 2017): ambulances were diverted, non-emergency surgeries, delayed; appointments, canceled; and phone lines and email accounts, inaccessible (Collier 2017; New Jersey Cybersecurity and Communications Integration Cell 2019). All told, the attack cost the National Health Service $118,588,000 in canceled appointments alone (What is WannaCry ransomware? n.d.). However, this financial loss pales in comparison to the total estimated cost of the WannaCry attack: $4 - 8 billion (Greenberg 2018).

The NotPetya attack followed WannaCry a month later, on the eve of Ukraine's Constitution Day. Created by a Russia-affiliated group named Sandworm, NotPetya also was a worm that encrypted users' files and used EternalBlue as an infection vector; however, unlike WannaCry, it is generally classified as a wiper, a type of malware that destroys its victims' files and devices, and was able to even infect patched computers by pulling the credentials needed to access and infect them from unpatched ones with another exploit named Mimikatz. Earlier that year, Sandworm had infiltrated Linkos Group's update servers and created a backdoor through the latter's widely popular M.E.Doc tax accounting software into any computer with M.E.Doc installed (Greenberg 2018). Those compromised computers then became NotPetya's first victims when it launched on June 27, 2017. Affected systems displayed an extortion message that demanded payment for a decryption key; however, despite the initial belief that NotPetya was ransomware, payments did not result in the release of the key—in fact, a decryption key was never found nor was it ever possible for the attackers to generate one (Ivanov and Mamedov 2017).

Although NotPetya had a larger total estimated cost at $10 billion (Greenberg 2018), its spread appears to have been more targeted than WannaCry: as much as 60 - 80% of the attacks occurred in Ukraine, followed by 30% in Russia, with the next-most infected countries being Poland, Italy, and Germany (Satter and Bajak 2017; Shea 2017). However, that is not to suggest its effects were any less severe. Not only did the attack disable large swaths of Ukraine's critical infrastructure, including 90% of Ukraine's second-largest bank, it also affected "practically every federal agency," leading to the Ukrainian government being described as functionally "'dead'" by its minister of infrastructure (Greenberg 2018). Although some companies lost millions due to damages, individuals not directly impacted by the attack felt second-order effects, such as shipping delays and traffic jams, reduced hospital operational speeds due to the loss of transcription services, and the inability to withdraw cash or purchase certain drugs

(Greenberg 2018; Greenberg 2019). It bears noting that it took the U.S. seven months from the time of WannaCry's occurrence to officially attribute it to a threat actor, and it took eight months in the NotPetya case (Executive Office of the President 2017, 2018).

Applying the 2018 NPR to WannaCry and NotPetya

Superficially, NotPetya and WannaCry seem to match many of the conditions laid out by the Trump NPR. For example, as discussed prior, the inclusion of non-nuclear attacks which "include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure" was one of the most significant changes to the U.S.' nuclear posture introduced by the Trump administration. The WannaCry and NotPetya attacks meet this criterion, both with regards to being attacks on the U.S., its allies, or partners, as well as being ones that affected their infrastructure. The U.S. Cybersecurity and Infrastructure Security Agency recognizes sixteen sectors as critical infrastructure, including healthcare, energy, financial services, and transportation, the latter of which also includes aviation, postal, and shipping. WannaCry's effect on Britain, one of the U.S.' closest allies, as well as Taiwan, a recognized U.S. partner (U.S. Department of State 2022), have already been detailed. Another notable victim of the two attacks, and among the countries most severely affected by them (Perlroth and Sanger 2017), was Ukraine, which has been a partner with the U.S. since the 1990s through the DoD's State Partnership Program and NATO's Partnership for Peace (North Atlantic Treaty Organization 2022; U.S. Department of State 2023). Notably, as a result of the NotPetya attack, four Kiev hospitals, six power companies, two airports, over 22 Ukrainian banks, and even the computers monitoring radiation levels at Chernobyl were forced to shut down, leaving many Ukranians unsure if they would be able to withdraw cash and refill their cars, purchase food, or refill prescriptions (Greenberg 2018).

Though the U.S.' Homeland Security Department initially said that the number of WannaCry victims in the U.S. was "'very small'" (Chappell 2017) and later reports indicate that the timely discovery of a kill switch prevented WannaCry from spreading far in the U.S. (Satran 2017), that does not mean that the U.S. was removed from feeling WannaCry's effects: a local Memphis newspaper reported that over a hundred FedEx flights suffered delays at the time of the WannaCry (Risher 2017). Likewise, when NotPetya struck, almost a quarter of all shipping terminals owned by Maersk, the world's largest shipping company at the time, were offline and experiencing miles' worth of traffic jams (Greenberg 2018). In this respect, NotPetya and WannaCry posed a challenge to the U.S.' vital interest in protecting "the homeland, the American people, and the American way of life," under which the mission to "protect our critical infrastructure and go after malicious cyber actors" was nested (Trump 2017).

Additionally, the NPR states that "Extreme circumstances could include significant non-nuclear strategic attacks," and despite the administration's definition of "significant" being left ambiguous, it is difficult to understate how influential and large-scale WannaCry and NotPetya were. At the time of their occurrence, they were considered the two most virulent, wide-reaching, and costliest cyberattacks ever (Scott and Wingfield 2017; Tatar et al 2021; Volz 2017), and, with regards to NotPetya, the severity of its effects was acknowledged by the U.S., United Kingdom, and Ukrainian governments and its officials. The former released an official statement calling NotPetya "the most destructive and costly cyber-attack in history" (Executive Office of the President 2018), while an advisor to Ukraine's interior minister called the attack "the worst in

Ukraine's history" (Prentice 2017).[1] Likewise, the Trump administration's former Homeland Security Advisor later compared the effects of NotPetya to "'using a nuclear bomb to achieve a small tactical victory'" (Greenberg 2018), and the then-British Minister for Cyber said in no uncertain terms that WannaCry was "one of the most significant to hit the UK in terms of scale and disruption" (Foreign & Commonwealth Office and Ahmad of Wimbledon 2017). Besides the attacks' extraordinary technical and historical nature, cybersecurity experts also feared that their ability to self-propagate represented a watershed for ransomware attacks, being akin to the "atom bomb" of such attacks (Perlroth and Sanger 2017). As such, both the content and quantity of statements related to the unprecedented nature of WannaCry and NotPetya are testament to their significance to government officials and industry professionals.

Besides threatening the first pillar of U.S. vital interests, the damage these two attacks inflicted also posed a challenge to the U.S.' promotion of American prosperity, which includes the mission to "protect data and underlying infrastructure" (Trump 2017). Since the NSS's release, the Trump administration has come to summarize this pillar as "Economic security is national security" (Hendry 2017), the former of which relies upon the "flow of goods and services, people and capital, and information and technology across our borders" (U.S. Department of Homeland Security 2022). This precious flow of resources was stopped in multiple places and times as a result of NotPetya and WannaCry. Besides the previously-mentioned shipping delays that Maersk and FedEx both experienced (in the latter's case, both in May and June that year), NotPetya also shut down New Jersey-based pharmaceutical giant Merck's vaccine-manufacturing facilities to such an extent that the global supply for the leading

[1] At the time of the source's writing, the attack was attributed to either Cryptolocker or "a version of the WannaCry ransomware"; however, given the lack of corroborating evidence and the timing and circumstances of the statement, this attribution is believed to be erroneous.

vaccine for human papillomavirus that year had to be supplemented by the U.S.' entire emergency cache; afterwards, Merck needed eighteen months to refill the stockpile with the 1,800,000 doses it had borrowed (Voreacos et al 2019).

In addition to goods, NotPetya also led to the destruction of countless computers and data. Merck alone lost 30,000 devices, 7,500 servers, and, in one researcher's case, fifteen years of work due to NotPetya (Voreacos et al 2019), whereas Mondelez, a food company based in Chicago, lost 24,000 laptops and 1,700 servers (Satariano and Perlroth 2019). Finally, as noted prior, although the number of computers affected by WannaCry was estimated at 300,000, and the malware was capable of rendering devices permanently inoperable by permanently encrypting them, public information on exactly how many devices U.S. companies lost could not be located. In short, an argument could be made that these attacks, particularly NotPetya, did threaten multiple U.S. vital interests.

Yet, despite the ways the Trump NPR ostensibly matches these two cyberattacks, there are just as many caveats to them. For example, to Ukraine, the NotPetya attack must have surely demonstrated elements of an attempted strategic attack, given that all of the Ukrainian government's networks—including, presumably, the Ministry of Defence—and about 10% of all computers nationwide were inoperable (Brewster 2017; Greenberg 2018; Кабачинський 2017), making it difficult for the national government to fulfill its day-to-day functions. However, there are two details related to the attack that suggest NotPetya posed a limited threat to Ukraine's centers of gravity. First, though it is indisputable that Ukraine's critical infrastructure was threatened, the precise sectors involved—largely energy, financial services, and transportation—are not directly tied to a country's warfighting ability. Although their loss would have doubtless had a negative effect on Ukraine's economic security and its public health—two of the named potential “debilitating effects” that the loss of a critical infrastructure may have on a country (U.S. Cybersecurity and Infrastructure Security Agency 2020)—as gas tanks emptied and citizens ran out of prescription drugs, it is difficult to imagine Ukraine’s military immediately losing its freedom of action, physical strength, or will to fight as a result. Moreover, Ukrainian energy companies infected by NotPetya reported that they were largely “unaffected” by the attack and were able to continue providing power (Brewster 2017), further diminishing the risk that NotPetya could have posed on Ukraine’s centers of gravity.

Second, as with WannaCry, NotPetya was short-lived. Both attacks lasted approximately a day before they were stopped. A cybersecurity researcher managed to neutralize WannaCry on May 13, 2017 by activating a kill switch that he had accidentally discovered after registering a domain queried by the ransomware (Hutchins 2017), while NotPetya required the intervention of the Ukrainian government, which confirmed in a blog post that NotPetya had been “halted” (Odell and Jones 2017). The ephemeral nature of these attacks helped to contain the spread and, therefore, the destructiveness of both malware, as evidenced by the earlier discussion about how little WannaCry affected the U.S. compared to other countries. Similarly, considering the sectors NotPetya targeted and how it was only active for a day, the attack only fit the definition of a strategic attack in the loosest sense of the term, a fact made all the more notable by the significant difference between both cyberattacks’ durations and the months needed for the U.S. to attribute them.

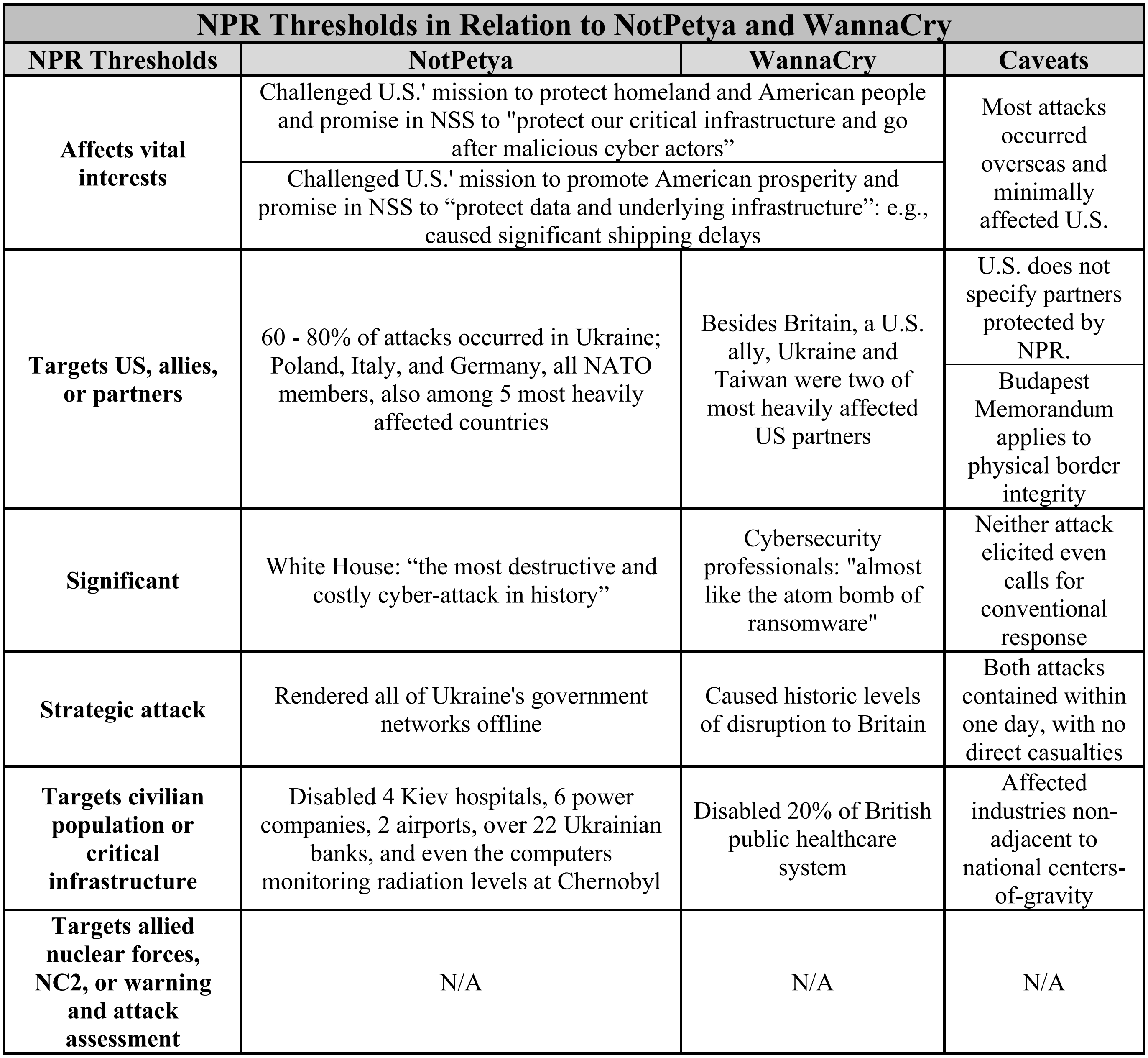
It is even more difficult to assert that the U.S. was at risk of a strategic loss. True, there were reports that the U.S. suffered significant shipping delays because of the attacks, and some hospitals in Pennsylvania were admittedly reduced to operating with paper and pencils due to the loss of the Nuance transcription service (Greenberg 2019). However, the shipping delays appeared to mostly involve commercial and perishable goods, and no reports were ever released attributing lives lost to either cyberattack, despite both affecting healthcare services. In fact, the first attributable death to a cyberattack would not occur for at least another three years (Eddy and Perlroth 2020). This evidence suggests both WannaCry and NotPetya lacked permanent effects outside of economic and information loss, and it potentially explains why, despite the American public generally being more willing to support retaliating against cyberattacks on critical infrastructure or NC3 architecture (Kreps and Schneider 2019; Schneider 2020), no such calls seem to have reached American policymakers.

Moreover, the extent to which the NPR applies to U.S. partners is ambiguous. This ambiguity means it remains unclear how much the U.S. would prioritize its autonomy over intervening on a partner's behalf. After all, although both Britain and Ukraine have long relationships with the U.S., a minimal U.S. response to WannaCry on Britain's behalf could be explained by the fact that effects concentrated in a hospital system are unlikely to generate strategic results. Such an explanation is more difficult to apply to Ukraine and NotPetya; however, the Budapest Memorandum provides some clues. Through the Memorandum, the U.S. made security assurances to protect Ukraine in the event that Russia failed to " respect the independence and sovereignty and the existing borders of Ukraine," did not "refrain from the threat or use of force," and failed to ensure "that none of their weapons will ever be used against Ukraine except in self-defense" or according to the United Nations' charter (No. 52241. Ukraine, Russian Federation, United Kingdom of Great Britain and Northern Ireland and United States of America 2021). Disabling the government's networks may have posed a threat to Ukraine's domestic sovereignty, but there are no reports of NotPetya generating kinetic effects, and because the attack was believed to have been state-sponsored, it could be argued that Russia did not conduct the attack *per se*. Together, technicalities such as these limit the available options for retaliation, as an unrestrained response against adversaries within another country's territory risks angering the host country.

Nuclear attacks are also politically costly, given the taboo surrounding their use (Pant 2012; Tannenwald 1999). A nuclear response to an attack akin to NotPetya or WannaCry, for all the rhetoric surrounding how significant or akin to tactical nuclear bombs that they might have been, would have been grossly disproportionate, particularly considering no lives were lost and that even low-yield nuclear weapons are "thousands of times more destructive than the largest conventional ones" and risk years of radiological contamination (Mount 2018). In short, with the aforementioned lack of public outcry pressuring U.S. politicians to respond violently to WannaCry and NotPetya, there would actually have been strong disincentives against responding with nuclear weapons. Therefore, given the circumstances of NotPetya and WannaCry, had the Trump NPR been in effect, the U.S. likely would have had strong reasons to take advantage of the NPR's ambiguity and rule out a nuclear response.

In the context of U.S. cyber deterrence in general, these gaps suggest the threat of nuclear retaliation has little deterrent effect in the cyber domain. Despite NotPetya and WannaCry being two of the most virulent and costliest cyberattacks to date, they still failed to meet crucial thresholds set forth by the Trump NPR and did not evoke even a conventional military response. These findings are summarized in Figure 1 alongside select key data, and they suggest that most other attacks—which tend to be of smaller scale and costliness—will likewise fail to meet the thresholds. Specifically, they could not definitively constitute a strategic threat to the U.S. or its allies or partners, even though they were significant attacks that threatened two of the U.S.' vital interests and affected both civilians and critical infrastructure. Therefore, both cases are evidence of some of the popular claims found in the literature regarding the thresholds cyberattacks would need to cross in order to result in violence: they demonstrate how the sabotage (i.e., impairment) of technical systems and “things” are unlikely to lead to a violent response (Rid 2012; Rid 2013), individuals tend to demonstrate greater restraint when considering the possibility of retaliating with force (Kreps and Schneider 2019), particularly if the response is made following a significant delay after the event occurs (Brantly 2018); and there likely needs to be a certain level of physical violence or horror that can evoke public outcry for cyberattacks to merit a kinetic response (Borghard and Lonergan 2019). Thus, based on this study, a nuclear response would likely have been unthinkable—and it will likely remain unthinkable, even when attacks can be attributed—unless subsequent attacks succeed where NotPetya and WannaCry failed, namely by threatening U.S. vital interests for an extended period of time; demonstrably targeting critical infrastructure *and* generating permanent, if not violent, effects; and affecting the U.S. or an ally or partner to whom the U.S. has such clear security commitments to that ignoring such a significant attack incurs greater cost than addressing it.

Figure 1: Summary of Findings



NPR Thresholds in Relation to NotPetya and WannaCry			
NPR Thresholds	**NotPetya**	**WannaCry**	**Caveats**
Affects vital interests	Challenged U.S.' mission to protect homeland and American people and promise in NSS to "protect our critical infrastructure and go after malicious cyber actors"		Most attacks occurred overseas and minimally affected U.S.
	Challenged U.S.' mission to promote American prosperity and promise in NSS to "protect data and underlying infrastructure": e.g., caused significant shipping delays		
Targets US, allies, or partners	60 - 80% of attacks occurred in Ukraine; Poland, Italy, and Germany, all NATO members, also among 5 most heavily affected countries	Besides Britain, a U.S. ally, Ukraine and Taiwan were two of most heavily affected US partners	U.S. does not specify partners protected by NPR.
			Budapest Memorandum applies to physical border integrity
Significant	White House: "the most destructive and costly cyber-attack in history"	Cybersecurity professionals: "almost like the atom bomb of ransomware"	Neither attack elicited even calls for conventional response
Strategic attack	Rendered all of Ukraine's government networks offline	Caused historic levels of disruption to Britain	Both attacks contained within one day, with no direct casualties
Targets civilian population or critical infrastructure	Disabled 4 Kiev hospitals, 6 power companies, 2 airports, over 22 Ukrainian banks, and even the computers monitoring radiation levels at Chernobyl	Disabled 20% of British public healthcare system	Affected industries non-adjacent to national centers-of-gravity
Targets allied nuclear forces, NC2, or warning and attack assessment	N/A	N/A	N/A

Conclusion

In spite of the rivers of ink spilled discussing the relationship between cyberattacks and nuclear deterrence, few studies have undertaken the task of examining the reverse—that is, how nuclear retaliation might influence cyber deterrence, if at all—even though the U.S. nuclear posture under the Trump administration took the extraordinary step of enshrining the possibility of a nuclear response to non-nuclear strategic attacks. Inspired, therefore, by the work of Rid (2012) and Kreps and Schneider (2019), I offer one of the few attempts to explicitly scrutinize the role that nuclear weapons use may play in deterring cyberattacks.

Bearing in mind that WannaCry and NotPetya are two of the most widespread and costliest cyberattacks to date and yet both failed to elicit even conventional military responses (therefore providing upper bounds for what cyberattacks can accomplish without violent retaliation), I provided a case study analyzing the events and effects of NotPetya and WannaCry and how they do and do not match the language of the Trump administration's NPR. The logic behind this design being the NPR precedes a nuclear response on the causal chain: if it fails to meet the NPR's standards, it can reasonably be assumed that the administration would rule out nuclear weapons. To provide my analysis, I drew on both primary and secondary information about the attacks from official government publications and announcements, international organizations, newspapers, cybersecurity organizations, and, sparingly and where appropriate, think tanks. Specifically, I argued that a traditional nuclear deterrent has little effect on a state's ability to deter cyberattacks because the threat lacks credibility: most known cyberattacks—even ones as infamous as NotPetya and WannaCry—only generate intangible, impermanent, and, ultimately, transient losses, usually in the form of economic and data-related losses. As a result, they struggle to qualify as a strategic attack, in turn making it difficult for the U.S. to justify the political costs of nuclear weapons use.

These findings have important ramifications on the theoretical thinking behind cyber and nuclear policy. First, they demonstrate how states require a significant amount of time to attribute a cyberattack, are likely more hesitant to resort to punishment, and, particularly in the case of state-sponsored attacks, are limited in their decision space by the operational realities of trying to reach adversaries, whose identities and relationships states can never be fully certain about, across national borders. That is, these two cases are real-world illustrations of some of the ways that deterrence in cyberspace differs from deterrence in the physical domains. Second, in drawing attention to these gaps between deterrence posture and reality, they also raise normative questions that U.S. policymakers must eventually contend with, namely, whether the ability to threaten a nuclear response necessarily means it is an effective one for cyber deterrence—and whether it should be used at all. Finally, and relatedly, they underscore the need for clearer conceptions of proportionality in cyber deterrence thinking: while it can be reasonably assumed government organs would be inflammatory targets, what of civilian industries and their relationship to a state's war-fighting ability? Both WannaCry and NotPetya affected U.S., allied, and partnered critical infrastructure, but, as mentioned, the sectors had few apparent ties to military power. Had it targeted military-related sectors, though, would the loss of a defense contractor be commensurate with the loss of a non-defense-related government agency? If effective deterrence hinges upon clear and consistent communication of red lines and consequences, it is important that the deterring state be able to consistently determine what it values more. Put simply, as-is, U.S. cyber deterrence policy remains a blunt instrument.

Two limits to this study bear acknowledgement. First, this design suffers from the fact that it is retrospective. Though it is highly doubtful that the Trump administration would have chosen a different course of action, even with the additional policy breadth provided, there is nevertheless an irrefutable nonzero chance that it *may* have acted differently with the policy backing. By design, this is unavoidable, but this shortcoming could be mitigated by examining only those cyberattacks that occurred after the Trump administration released its NPR. However, that option suffers from the problem of then having attacks of inadequate scale. Second, many aspects of the decision-making surrounding nuclear weapons happens behind closed doors, and cyber itself is a domain that is more difficult for the general public to observe—if a rocket is launched or explodes, a satellite might capture the image, despite not being party to the incident; when a cyberattack occurs, without technical know-how, most of the incident's events are contained to the attacker's and the screens of the victim(s). In other words, though every effort was made to collect a breadth of information related to WannaCry and NotPetya, this project ultimately relies on open sources, so those with more resources and better access to more privileged documents may be able to uncover new details that may well shift this study's findings.

Considering these limitations, the opportunities for future scholarship abound. As this paper is a qualitative case study, it would greatly benefit from an empirical and, preferably, quantitative analysis of the research question. One potential design is establishing a war game with two teams in which one side conducts a cyber campaign and sends increasingly destructive and fatal cyberattacks on the other side's country and noting when, if ever, the defending team finally turns to low-yield nuclear weapons. For additional research utility, some of the cyberattacks might be patterned off historical ones (e.g., Stuxnet, NotPetya, Colonial Pipeline, etc). Another game could be run with a similar setup, but instead of increasingly severe attacks, the attackers specifically select different sectors with increasingly more tangible ties to the military and, eventually, NC3. Alternatively, given the role of allies and partners in determining U.S. nuclear use per the NPR, it would be useful to know on which partners' and allies' behalf the American public would be willing to support nuclear use, if any, in response to a cyberattack. In that case, even a survey or interview format would be possible. Lastly, though it did not have as significant a focus in this paper, it would be useful to know whether there is a temporal limit on when a nuclear response to a catastrophic strategic cyberattack is permissible—that is, assuming nuclear use *was* justifiable, how long would it be so?

NPRs are a delicate balancing act between strategic ambiguity on the one hand and clarity of language on the other: too much clarity, and adversaries can more easily avoid inadvertent nuclear escalation, but it comes at the cost of committing the U.S. to certain actions and risking gray-zone operations; too much ambiguity, and the reverse is true. Considering it is unlikely the threat of a nuclear deterrent has any impact on the U.S.' ability to deter cyberattacks, it appears nuclear policy under the Trump administration suffered from the former of the two problems, bringing with it all the potential to overextend the U.S. Thus, for those rare few politicians in Washington who are legitimately interested in crafting effective policy, this research suggests the key to cyber deterrence lies elsewhere beyond the nuclear domain.

References

Acton, James M. 2018. "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War." *International Security* 43(1): 56–99.

Acton, James M. 2020. "Cyber Warfare & Inadvertent Escalation." *Daedalus* 149(2): 133–49.

Betts, Richard K. 2002. "The Soft Underbelly of American Primacy: Tactical Advantages of Terror." *Political Science Quarterly* 117(1): 19–36.

Borghard, Erica D., and Shawn W. Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26(3): 452–81.

Borghard, Erica D., and Shawn W. Lonergan. 2019. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* 13(3): 122–45.

Brantly, Aaron F. 2018. "The Cyber Deterrence Problem." In *2018 10th International Conference on Cyber Conflict (CyCon)*, IEEE, 31–54.

Brenner, Bill. 2017. "WannaCry: The Ransomware Worm That Didn't Arrive on a Phishing Hook." *Naked Security*. https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/ (January 30, 2023).

Brewster, Thomas. 2017. "Another Massive Ransomware Outbreak Is Going Global Fast." *Forbes*. https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/ (February 6, 2023).

Brown, Seyom. 2018. "The Trump Administration's Nuclear Posture Review (NPR): In Historical Perspective." *Journal for Peace and Nuclear Disarmament* 1(2): 268–80.

Carlino, Michael A. 2002. "The Moral Limits of Strategic Attack." *The US Army War College Quarterly: Parameters* 32(1). https://press.armywarcollege.edu/parameters/vol32/iss1/3 (January 30, 2023).

Chappell, Bill. 2017. "WannaCry Ransomware: What We Know Monday." *NPR*. https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday (February 3, 2023).

Collier, Roger. 2017. "NHS Ransomware Attack Spreads Worldwide." *CMAJ : Canadian Medical Association Journal* 189(22): E786–87.

Dawkins, Jr and James C. 2009. *Rising Dragon: Deterring China in 2035:* Fort Belvoir, VA: Defense Technical Information Center. http://www.dtic.mil/docs/citations/ADA539881 (January 30, 2023).

Eddy, Melissa, and Nicole Perlroth. 2020. "Cyber Attack Suspected in German Woman's Death." *The New York Times*. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (February 6, 2023).

Executive Office of the President. 2017. "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – The White House." The White House. https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (February 19, 2023).

Executive Office of the President. 2018. "Statement from the Press Secretary." *The White House*. https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ (February 6, 2023).

"Finding the Kill Switch to Stop the Spread of Ransomware." https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0 (February 3, 2023).

Foreign & Commonwealth Office, and Tariq Ahmad of Wimbledon. 2017. "Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks." *GOV.UK*. https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks (February 6, 2023).

Gartzke, Erik, and Jon R. Lindsay. 2017. "Thermonuclear Cyberwar." *Journal of Cybersecurity*. https://academic.oup.com/cybersecurity/article/2996537/Thermonuclear (January 27, 2023).

Goodman, Will. 2010. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4(3): 102–35.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (January 30, 2023).

Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. 1st ed. Doubleday.

Hayes, Peter. 2018. "Trump and the Interregnum of American Nuclear Hegemony." *Journal for Peace and Nuclear Disarmament* 1(2): 219–37.

Hendry, Erica. 2017. "Read Trump's Full Speech Outlining His National Security Strategy." *PBS NewsHour*. https://www.pbs.org/newshour/politics/read-trumps-full-speech-outlining-his-national-security-strategy (February 6, 2023).

Hutchins, Marcus. 2017. "How to Accidentally Stop a Global Cyber Attacks." *MalwareTech*. https://malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html (February 6, 2023).

Iasiello, Emilio. 2013. "Cyber Attack: A Dull Tool to Shape Foreign Policy." In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, IEEE, 1–18.

Ivanov, Anton, and Orkhan Mamedov. 2017. "ExPetr/Petya/NotPetya Is a Wiper, Not Ransomware." *Securelist by Kaspersky*. https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ (January 30, 2023).

Jones, Sam, and Tim Bradshaw. 2017. "Global Alert to Prepare for Fresh Cyber Attacks." *Financial Times*. https://www.ft.com/content/bb4dda38-389f-11e7-821a-6027b8a20f23.

Klare, Michael T. 2019. "Cyber Battles, Nuclear Outcomes? Dangerous New Pathways To Escalation." *Arms Control Today* 49(9): 6–13.

Kreps, Sarah, and Jacquelyn Schneider. 2019. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics." *Journal of Cybersecurity* 5(1): tyz007.

Lange, Katie. 2018. "National Defense Strategy: Alliances and Partnerships." *U.S. Department of Defense*. https://www.defense.gov/News/Feature-Stories/story/Article/1656016/national-defense-strategy-alliances-and-partnerships/https%3A%2F%2Fwww.defense.gov%2FNews%2FFeature-Stories%2FStory%2FArticle%2F1656016%2Fnational-defense-strategy-alliances-and-partnerships%2F (January 30, 2023).

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND.

Liff, Adam P. 2012. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies* 35(3): 401–28.

Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22(3): 365–404.

Lindsay, Jon R., and Erik Gartzke. 2019. “Introduction: Cross-Domain Deterrence, from Practice to Theory.” In *Cross-DOmain Deterrence: Strategy in an Era of Complexity*, eds. Jon R. Lindsay and Erik Gartzke. New York, NY: Oxford University Press.

Lindsay, Jon R., and Erik Gartzke. 2022. “Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains.” *Journal of Strategic Studies* 45(5): 743–76.

Lonsdale, David J. 2018. “Warfighting for Cyber Deterrence: A Strategic and Moral Imperative.” *Philosophy & Technology* 31(3): 409–29.

Lupovici, Amir. 2011. “Cyber Warfare and Deterrence: Trends and Challenges in Research.” *Military and Strategic Affairs* 3(3). https://www.inss.org.il/wp-content/uploads/2017/02/FILE1333533336-1.pdf.

MacKenzie, Peter. 2019. *WannaCry Aftershock*. Sophos. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf.

Mallory, King. 2018. *New Challenges in Cross-Domain Deterrence*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE259.html (January 30, 2023).

McNeil, Adam. 2017. "How Did the WannaCry Ransomworm Spread? | Malwarebytes Labs." *Malwarebytes*. https://www.malwarebytes.com/blog/news/2017/05/how-did-wannacry-ransomworm-spread (January 30, 2023).

Mount, Adam. 2018. "Trump's Troubling Nuclear Plan." *Foreign Affairs*. https://www.foreignaffairs.com/united-states/trumps-troubling-nuclear-plan (February 6, 2023).

New Jersey Cybersecurity and Communications Integration Cell. 2019. "NJCCIC Threat Profile WannaCry." *New Jersey Cybersecurity and Communications Integration Cell*. https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/wannacry (January 30, 2023).

"NHS Cyber-Attack: No 'second Spike' but Disruption Continues." 2017. *BBC News*. https://www.bbc.com/news/uk-39918426 (January 30, 2023).

"No. 52241. Ukraine, Russian Federation, United Kingdom of Great Britain and Northern Ireland and United States of America." 2021. In *Treaty Series 3007*, United Nations Treaty Series, United Nations, 167–82. https://www.un-ilibrary.org/content/books/9789214030966c009 (February 6, 2023).

North Atlantic Treaty Organization. 2022. “Relations with Ukraine.” *NATO*. https://www.nato.int/cps/en/natohq/topics_37750.htm (February 3, 2023).

Nye Jr, Joseph S. 2011. *Nuclear Lessons for Cyber Security:* Fort Belvoir, VA: Defense Technical Information Center. http://www.dtic.mil/docs/citations/ADA553620 (January 30, 2023).

Odell, Mark, and Same Jones. 2017. “Cyber Attack Hunt Focuses on Initial Ukraine Infection.” *Financial Times*. https://www.ft.com/content/0ead41a6-5bdb-11e7-b553-e2df1b0c3220.

Pant, Harsh V., ed. 2012. “The Nuclear Taboo.” In *Handbook of Nuclear Proliferation*, London: Routledge, 376. https://www.taylorfrancis.com/books/edit/10.4324/9780203840849/handbook-nuclear-proliferation-harsh-pant?refId=580901fc-7fb3-4026-a677-728a857f5902&context=ubx.

Péczeli, Anna. 2018. “The Trump Administration’s Nuclear Posture Review: Back to Great Power Competition.” *Journal for Peace and Nuclear Disarmament* 1(2): 238–55.

Perlroth, Nicole, and David E. Sanger. 2017. “Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool.” *The New York Times*. https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html (February 2, 2023).

Prentice, Alessandra. 2017. “Ukraine Official Says Version of WannaCry Virus Caused Cyberattacks.” *Reuters*. https://www.reuters.com/article/cyber-attacks-ukraine-rassomware-idUSS8N1GY03M (February 6, 2023).

Rid, Thomas. 2012. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35(1): 5–32.

Rid, Thomas. 2013. “More Attacks, Less Violence.” *Journal of Strategic Studies* 36(1): 139–42.

Risher, Wayne. 2017. “Memphis Hub IT Outage Could Slow FedEx Shipments.” *The Commercial Appeal*. https://www.commercialappeal.com/story/money/industries/logistics/2017/05/02/memphis-hub-outage-could-slow-fedex-shipments/101200988/ (February 3, 2023).

Satariano, Adam, and Nicole Perlroth. 2019. “Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.” *The New York Times*. https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html (February 6, 2023).

Satran, Richard. 2017. “ANALYSIS: WannaCry Attack Shows Trend toward ‘economic’ Cyber Threats, Rising Regulatory Risk.” *Reuters*. https://www.reuters.com/article/bc-finreg-cyber-threats-wannacry-idUSKBN19C2RU (February 3, 2023).

Satter, Raphael, and Frank Bajak. 2017. “New Cyberattack Wallops Europe; Spreads More Slowly in US.” *AP NEWS*. https://apnews.com/article/ap-top-news-international-news-technology-russia-business-57bb0af7145e4aefbe050b33636a15cf (January 30, 2023).

Schelling, Thomas C. 1966. *Arms and Influence*. Yale University Press.

Schneider, Jacquelyn. 2020. “A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem.” *The Washington Quarterly* 43(2): 159–75.

Scott, Mark, and Nick Wingfield. 2017. “Hacking Attack Has Security Experts Scrambling to Contain Fallout.” *The New York Times*.

https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html (February 6, 2023).

Scouras, James, Smyth, Edward, and Mahnken, Thomas. 2014. *Cross-Domain Deterrence in US–China Strategy*. Laurel, Maryland: The Johns Hopkins University Applied Physics Laboratory. https://www.jhuapl.edu/Content/documents/CrossDomainWeb.pdf.

Shea, Jamie. 2023. “How Is NATO Meeting the Challenge of Cyberspace?” (2).

Soesanto, Stefan, and Max Smeets. 2021. “Cyber Deterrence: The Past, Present, and Future.” In *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, NL ARMS, eds. Frans Osinga and Tim Sweijs. The Hague: T.M.C. Asser Press. https://link.springer.com/10.1007/978-94-6265-419-8 (January 30, 2023).

Spector, Leonard. 2022. “Cyber Offense and a Changing Strategic Paradigm.” *The Washington Quarterly* 45(1): 38–56.

Sterner, Eric. 2011. “Retaliatory Deterrence in Cyberspace.” *Strategic Studies Quarterly* 5(1): 62–80.

Stevenson, Jonathan, ed. 2018. “The Trump Administration’s Nuclear Posture Review.” *Strategic Comments* 24(2): vii–ix.

Tannenwald, Nina. 1999. “The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use.” *International Organization* 53(3): 433–68.

Tannenwald, Nina. 2005. "Stigmatizing the Bomb: Origins of the Nuclear Taboo." *International Security* 29(4): 5–49.

Tatar, Unal, Brian Nussbaum, Yasir Gokce, and Omer F. Keskin. 2021. "Digital Force Majeure: The Mondelez Case, Insurance, and the (Un)Certainty of Attribution in Cyberattacks." *Business Horizons* 64(6): 775–85.

Thieret, Jeffrey E, Steven J DePalmer, Frederick I Guendel, Jr., and Michael A Silver. 1996. *Hit'em Where It Hurts: Strategic Attack in 2025*. https://apps.dtic.mil/sti/citations/ADA333300 (January 30, 2023).

Tor, Uri. 2017. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40(1–2): 92–117.

Trump, President Donald J. 2017. *The National Security Strategy of the United States of America*. Washington, D.C.: The White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

"U.S. Blames North Korea for 'WannaCry' Cyber Attack." 2017. *Reuters*. https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q (February 6, 2023).

U.S. Cybersecurity and Infrastructure Security Agency. 2020. "Critical Infrastructure Sectors | CISA." *United States Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/critical-infrastructure-sectors (February 6, 2023).

U.S. Department of Defense. 2010. *2010 Nuclear Posture Review Report*. Washington, D.C. https://dod.defense.gov/Portals/1/features/defenseReviews/NPR/2010_Nuclear_Posture_Review_Report.pdf.

U.S. Department of Defense. 2018. *2018 Nuclear Posture Review Report*. Washington, D.C. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

U.S. Department of Homeland Security. 2022. "Trade and Economic Security | Homeland Security." *United States Department of Homeland Security*. https://www.dhs.gov/topics/trade-and-economic-security (February 6, 2023).

U.S. Department of Justice. 2018a. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." *United States Department of Justice*. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (January 30, 2023).

U.S. Department of Justice. 2018b. (United States District Court for the Central District of California) *United States of America v. Park Jin Hyok*.

U.S. Department of State. 2022. "U.S. Relations With Taiwan." *United States Department of State*. https://www.state.gov/u-s-relations-with-taiwan/ (March 6, 2023).

U.S. Department of State. 2023. "U.S. Security Cooperation with Ukraine." *United States Department of State*. https://www.state.gov/u-s-security-cooperation-with-ukraine/ (February 3, 2023).

Voreacos, David, Katherine Chiglinsky, and Riley Griffin. 2019. “Merck Cyberattack’s $1.3 Billion Question: Was It an Act of War?” *Bloomberg.com*. https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war (February 6, 2023).

WannaCry Ransomware Infection Heat Map. 2017. https://www.youtube.com/watch?v=IEAtGCkbq5Y (January 30, 2023).

“What Was WannaCry? | WannaCry Ransomware.” *Malwarebytes*. https://www.malwarebytes.com/wannacry (January 30, 2023).

Wilner, Alex S. 2020. “US Cyber Deterrence: Practice Guiding Theory.” *Journal of Strategic Studies* 43(2): 245–80.

Кабачинський, Ілля. 2017. “Вирус Petya заразил 12 500 компьютеров только в Украине. Пострадавшие есть в 64 странах.” *AIN.UA*. https://ain.ua/ru/2017/06/28/virus-petya-zarazil-12500-kompyuterov-tolko-v-ukraine-postradavshie-est-v-64-stranax/ (February 6, 2023).