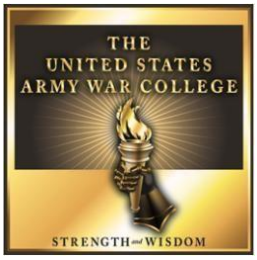
Strategy Research Project

Is the U.S. Being Deterred in Cyberspace?

by

Ms. Dawn A. Hicks
Defense Intelligence Agency

Under the Direction of:
Dr. William G. Pierce



United States Army War College
Class of 2018

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2018	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Is the U.S. Being Deterred in Cyberspace?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ms. Dawn A. Hicks
Defense Intelligence Agency

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. William G. Pierce

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
I understand this document will be included in a research database and available to the public. Author: ☒

13. SUPPLEMENTARY NOTES
Word Count: 5116

14. ABSTRACT

This study examines ways to achieve deterrence in the cyber domain by comparing two different deterrence theories--deterrence by fear which is predicated on imposing costs, and deterrence by denial, which suggests denying benefits. It identifies four critical elements needed for denial-based deterrence and three elements required to achieve a fear-based deterrence in cyberspace. The study considers these two theories and their limitations against current cyber trends and the emerging threat landscape to determine which theory is most applicable in the cyber domain. Overall, the study found a one-size fits all cyber deterrence strategy is likely to prove ineffective and that elements of both theories must be customized to deter adversaries with varying cyber capabilities. Furthermore, the U.S. political will is insufficient to establish the credibility required for a fear-based deterrence strategy to be effective.

15. SUBJECT TERMS
Defense, Detection, Attribution, Threat Intelligence, Norms/Redlines, Retaliation, Credibility, Enforcement, critical networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	27	

Is the U.S. Being Deterred in Cyberspace?

(5116 words)

Abstract

This study examines ways to achieve deterrence in the cyber domain by comparing two different deterrence theories--deterrence by fear which is predicated on imposing costs, and deterrence by denial, which suggests denying benefits. It identifies four critical elements needed for denial-based deterrence and three elements required to achieve a fear-based deterrence in cyberspace. The study considers these two theories and their limitations against current cyber trends and the emerging threat landscape to determine which theory is most applicable in the cyber domain. Overall, the study found a one-size fits all cyber deterrence strategy is likely to prove ineffective and that elements of both theories must be customized to deter adversaries with varying cyber capabilities. Furthermore, the U.S. political will is insufficient to establish the credibility required for a fear-based deterrence strategy to be effective.

Is the U.S. Being Deterred in Cyberspace?

Introduction

Cyber is changing the character of war at the speed of technology and with it, decision-makers and academics alike continue to debate cyber deterrence. Some believe deterrence is an escalatory concept of the past that has no place in the cyber domain while others believe a cyber deterrence policy is crucial for U.S. national defense. Regardless of one's position, the cyber domain is uniquely complex, and it is not unusual that strategic leaders question the definition of and the methods to accomplish cyber deterrence. The initial reaction by most is to apply the same Cold war, nuclear deterrent strategies against cyber threats. However, the nuances presented by cyber activity as an instrument of war distinguishes 21st century warfare from the past and therefore demands a significantly different approach. This study examines ways to achieve deterrence in the cyber domain by comparing two different deterrence theories – deterrence by fear which is predicated on imposing costs and deterrence by denial which suggests denying benefits. Informed by industry experts, this study identifies four critical elements needed for denial-based deterrence and three elements required to achieve a fear-based deterrence in cyberspace. The study considers the merits and the limitations of the two theories against current cyber trends and the emerging threat landscape to determine which is most applicable for the cyber domain. Comparing elements of deterrence by fear and deterrence by denial provides strategic leaders with a foundational understanding of the complexities of the cyber domain.[1]

Key Findings

- Deterrence strategies must align to individual adversaries

- Current political will is not credible enough to deter adversaries in cyberspace
- Robust cyber deterrence must include elements of denial and fear
- Cyber events affecting civilian populations will increase demand for retaliation
- Deterrence by fear encourages adversaries to increase offensive cyber capabilities
- U.S. networks must be prioritized in terms of criticality

Traditional Deterrence Theory

Early theories of deterrence suggest a state's power lies with its ability to discourage, by means of credible threat and willingness to punish, potential adversaries from choosing war as a course of action. While traditional fear-based deterrence theory is an effective way of deterring peer competitors, its limitations may result in unintended consequences. For example, fear-based deterrence might encourage an arms race or create a permissive environment for escalation and miscalculation, notwithstanding the security implications of revealing significant capabilities.

There are two primary ways to deter an adversary, through fear or denial. First, deterrence by fear promises a potential adversary a retaliation so costly that the benefits of action are less than the price of retaliation.[2] This form of deterrence relies on pre-defined and articulated redlines that if crossed, the adversary should expect a retaliatory action. Second, 'deterrence by denial' seeks to complicate the enemy's ability to achieve objectives by ensuring the desired targets are impossible to seize, hold, or exploit.[3]

The Deterrence Operations-Joint Operating Concept (DO-JOC) offers a third approach to deterrence that encourages adversary restraint. This approach attempts to convince the adversary that inaction would result in acceptable outcomes. Convincing

an adversary that it will lose less by restraining its activity than by taking action may reveal to its policy makers that restraint is more beneficial. While this approach may prevent escalation in some cases, in others it only serves to embolden the adversary as they see no repercussion for their actions.[4]

For deterrence by fear to be effective, there must be a credible threat which lies in Washington's commitment to enforce violations of clearly articulated norms and redlines. Deterrence by fear also assumes adversaries are rational actors and will abandon escalatory intentions for fear of reprisal upon violating articulated norms or redlines. Achieving deterrence by fear also boils down to a competition of wills based on interests. If an adversary displays more resolve than the U.S. has in inflicting a punitive retaliation, deterrence by fear fails.[5]

In contrast, deterrence by denial does not require pre-defined norms and redlines, a rational adversary, or a credible promise of retaliation as a form of dissuasion. Deterrence by denial ensures desired networks are impossible to access and exploit.[6] This approach requires impenetrable defenses, strong enough to withstand the most capable adversaries. However, this is highly unlikely given countless potential access points into critical networks.

While deterrence aims to dissuade an adversary from taking an action not yet started, skeptics maintain a non-action cannot be proven as the result of a deterrent action. Regardless, it is plausible to assume the absence of deterrent efforts provides adversaries with greater freedom of action.[7]

Difference Between Nuclear and Cyber Deterrence

The U.S. and Russia effectively achieved nuclear deterrence by building their nuclear arsenals in the hopes both sides would refrain from attacking each other

because of the certainty of mutual assured destruction.[8] Nuclear deterrence by fear proved effective during the Cold War for two reasons. First, the U.S. clearly demonstrated its nuclear capability and willingness to use it during WWII against Japan, setting the precedent and establishing a credible threat. Second, established redlines and direct communication between the U.S. and Russia prevented catastrophic nuclear miscalculations.

In hindsight, deterrence in the nuclear era was relatively easy to attain compared to today as the landscape in the cyber domain is drastically different. The days of known adversaries, known capabilities, and known points of origin are over. During the Cold War, it was clear in the minds of policy makers what constituted an act of war. The cyber domain, however, blurs those lines and it is less clear what activities the U.S. should deter. Rapid globalization and adversaries possessing cyber capabilities on par with the U.S. are changing the character of the operational environment. Reliance on cyber technologies and the inter-connectedness of networks create a significant vulnerability to U.S. citizens, military, and critical infrastructure despite being at the forefront of cyber technology. Unlike nuclear capabilities of privileged states, a variety of underprivileged actors possess the capability to threaten U.S. interests through peripheral cyber means. State, non-state, criminal, and independent actors use cyber because of its low cost and low barriers to entry. There is often a lack of consequences due to fundamental challenges of attribution and lack of political will to respond to cyber events. Today, actor proliferation means more adversaries to deter and sophisticated state-actors employ cyber capabilities in the ambiguous grey-zone activity[9] avoiding tripwires that could result in a retaliatory action.[10]

During the Cold War, the Soviet Union was the singular nuclear-capable adversary to deter. Today, there are 4+1 cyber capable adversaries to deter (Russia, China, North Korea, Iran + violent extremist organizations) along with a host of cyber criminals and proxy actors, each with their own level of capability and intent.[11] As a result, applying deterrence theories to today's complex cyber domain requires one to erase every Cold War indicator previously relied upon, and consider an approach that combines both deterrence by fear – imposing unacceptable costs – and deterrence by denial – denying benefits of action. There are seven fundamental ways cyber warfare differs from traditional warfare.[12]

- Potential to cause damage more widespread than a physical attack
- Can occur almost instantaneously against any target in the world
- Capabilities are typically single-use
- Adversary intentions are unclear (espionage vs. offensive action)
- Rapid pace of technology advances
- Availability of malicious cyber technologies
- Vague or absent international laws

Different Adversaries Require Different Deterrence

Deterrence differs in various strategic and cultural contexts. Cyber actors have different motivations and degrees of cyber capabilities.[13] As a result, U.S. ability to deter each group of cyber adversaries will vary significantly and will require a more tailored approach taking into consideration an adversary's intent, will, effectiveness, and capabilities. For example, U.S. willingness to punish North Korea for attacking Sony pictures is different from its willingness to punish China for stealing proprietary defense-

related information.[14] Even though China's cyber espionage was costlier than the North Korean attack on Sony, the difference lies in intent. In its response to North Korea, the U.S. clearly signaled an unwillingness to tolerate an attack on freedom of speech.[15] However, through its soft response to China, the U.S. signaled tolerance and acceptance of cyber espionage, likely because U.S. espionage activities would also be subject to retaliation by China.[16]

To date, the U.S. reaction to cyber events has been too inconsistent to serve as a viable deterrent, leading many to question whether the U.S. possesses the political will to impose costs on adversaries such as Russia and China. In response to Russia's hacking of the Democratic National Committee, the U.S. based its response on the infringement of political sovereignty. Meanwhile, there was no U.S. response to the Iranian attack on Las Vegas Sands Corporation, which suffered damages equal to those suffered by Sony, according to cyber deterrence expert Dr. Martin Libicki.[17]

> The U.S. runs the risk of trivializing cyber-attacks, such as the denial of service attack against TV5Monde in France in April 2015 and the December 2015 and 2016 cyber-attacks against Ukraine's electrical power grid. Instead of retaliation, the U.S. labeled these events as "vandalism" and abstained from punishing the attackers. In response to such attacks, the United States often dithers on both a cyber and whole-of-government reply, thereby sending the message that such activities will not be met by any sort of robust, punitive U.S. or international response – cyber or otherwise.[18]

In response to perceived Russian influence during the 2016 U.S. presidential election, the Obama administration took a decidedly asymmetric response by expelling 35 Russian diplomats, closing two Russian compounds and sanctioning nine specific Russian entities and individuals. This focus was so narrow that the impact appeared deliberately soft and amounted to little more than a public hand slap.[19]

Overall, it is unlikely the administration's diplomatic actions will have any effect in deterring Russian cyber aggression in the future. If anything, Russia will likely become emboldened further by the relatively soft sanctions.[20] According to Michael McFaul, U.S. ambassador to Russia for the Obama administration from 2012 to 2014, "The punishment did not fit the crime." He added, "Russia violated our sovereignty, meddling in one of our most sacred acts as a democracy — electing our president. The Kremlin should have paid a much higher price for that attack. And U.S. policymakers now…should consider new actions to deter future Russian interventions."[21]

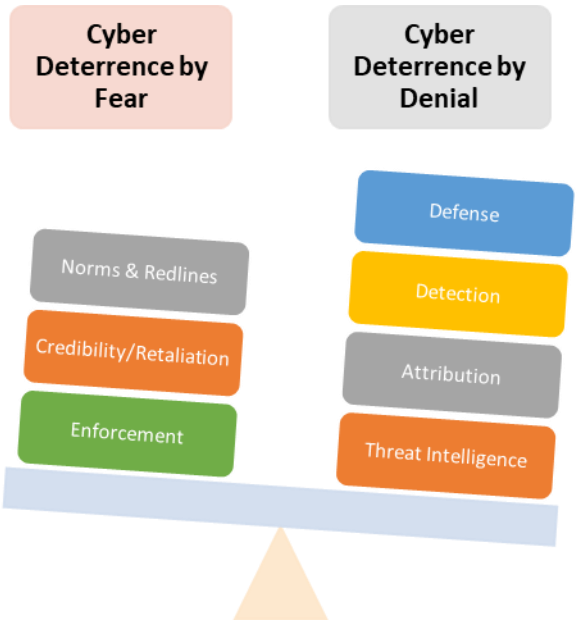


Figure 1. Elements of Cyber Deterrence[22]

A comprehensive cyber deterrence strategy requires elements of denial and fear, specifically increasing capability in seven critical areas. These elements are customized based on the threat and relative value of the networks. These areas include: defense, detection, attribution, threat intelligence, norms and redlines, credibility/retaliation, and enforcement. See Figure 1. Blindly applying a one size fits all strategy increases the likelihood of a failed overall cyber deterrence strategy. However, it is easier said than

done as each of these elements poses its own set of unique challenges and each is more suitable to deter a certain kind of adversary and a specific kind of threat. The next sections will examine each of the elements of cyber deterrence.

Denial-based Elements of Cyber Deterrence

Defense

Even with robust layered defense measures in place, the opportunity to gain access to a desired network is often greater than a defender's ability to protect it. As a result, a denial-based deterrence strategy aimed at bolstering defenses alone will likely continue to prove insufficient. Defensive measures such as firewalls, anti-virus, and good cyber security practices prevent passive and active cyber events. However, insider and close-access operations also pose a significant risk even when technical defenses are robust. This requires layered defenses, such as protecting data and passwords from disgruntled employees and safeguarding physical hardware such as server rooms from tampering. Distribution threats also pose a challenge to network defense. For example, compromised software updates can introduce backdoors into a critical network providing adversaries with access.[23] Increased network diversification, segmentation, and redundancies can reduce vulnerabilities in these areas.[24]

Detection

Detection differs from defense in that defensive measures prevent intrusions by actively filtering network traffic while detection passively detects system intrusions. Detection relies on a network of sensors monitoring networks for attack signatures used in previously logged attacks. Updated defenses are useful in detecting and alerting on known attack signatures. Unfortunately, previously undetected or unknown signatures or breeches resulting from insider operations can go undetected for minutes, days,

week, or years. It is the effect that usually indicates that an intrusion has occurred.[25] According to multiple cyber security companies, the time between a breach occurring and its detection averages 229 days[26] and most breaches are reported after stolen assets appear in the underground economy.[27] An attacker that is harder to detect, investigate, and remediate is inherently more likely to remain in an environment to accomplish their mission, resulting in theft of greater volumes of information or quiet network persistence that could enable data destruction, deletion, or manipulation.[28]

There is some utility in maintaining the ability to see an adversary but not immediately taking defensive measures. Detection can gain insight into adversary tactics, techniques, and procedures and it may also provide opportunities for denial and deception operations such as providing the adversary with tailored information or luring them into honeypots.[29]

Attribution

Attribution is a fundamental challenge in the cyber domain and using it to deter an adversary is complicated. Attributing cyber events is more than just tracing an event back to its point of origination. Although technical capabilities are getting better at identifying where cyber events originate, releasing attribution information publicly can undermine detection capabilities and future operations. Relying on technical evidence alone also fails to consider the geo-political factors and the risk of misattribution. Public attribution of malicious cyber events may prove effective at stopping an event in progress, but it does little to deter it before it occurs. For attribution to be a viable deterrent, there must be no doubt in an adversary's mind of U.S. ability to pinpoint with precision the origin of any cyber event along with a willingness to make it known in an effort to deter other actors. Given the current difficulties in attributing cyber events to

specific actors or countries, attribution as an element of deterrence should not be viewed as the most reliable element of a deterrent strategy.

Threat Intelligence

In addition to enhancing defense and detection capabilities, threat intelligence is the critical component that enables a truly proactive security posture and a threat hunting function. According to Mandiant, cyber threat intelligence helps organizations develop and maintain a data-driven and automated baseline threat profile that informs security teams of the most likely who, what, where, when, and how of the attacks and the best way to begin looking for them.[30] The use of cyber threat intelligence is critical for organizations to identify potential blind spots as threat actor techniques change, adding "Sophisticated intelligence integration, automation, and threat hunting should be the end-state goal for organizations facing significant exposure to cyber-attacks."[31] Threat intelligence can ultimately inform the design of a deterrence operation by informing who the likely actors are and determining whether they are more risk adverse or acceptant.

Fear-based Elements of Cyber Deterrence

Norms & Redlines

Deterrence by fear only works when cyber adversaries know in advance which actions may prompt a retaliatory response. Despite the efforts of the NATO Cyber Center of Excellence (NATO-CCOE), there are no internationally accepted norms and redlines in cyberspace. Regardless, global cyber actors are actively setting the precedent for future cyber operations through their current actions. As significant cyber operations continue to go unpunished, the U.S. will miss opportunities to shape and define norms and redlines. As a result, unpunished intrusions gain a level of

international tolerance which encourage adversaries to continue pushing boundaries resulting in escalating malicious cyber operations. According to former U.S. Cyber Command (USCYBERCOM) Commander, GEN Alexander, “The U.S. should seek to develop the rules of engagement now [in cyberspace], when things are relatively calm, rather than seeking to identify and create them during a crisis.”[32]

The goal is not to predict every possible doomsday scenario in cyberspace and make it off-limits. A cyber policy should start by articulating generally held norms and redlines. Without them, our adversaries become emboldened through trial and error, simply guessing which actions will illicit an international response and which ones will not. Further complicating matters, when the U.S. conducts malicious cyber activities, it likely sets a precedent in an adversary’s mind that certain behaviors are acceptable in cyberspace to protect national interests. Additionally, adversaries likely anticipate U.S. restraint and soft responses to cyber events when they are determining if the costs outweigh the benefits of any planned cyber operation. Until the world experiences a cyber event so catastrophic that it creates the political will to respond, countries will continue to look to one another to gauge what is acceptable and continue to incrementally test what kind of cyber activity generates an international response and just how large that response will be.

Retaliation & Credibility

For the U.S. to maintain the credible threat needed for an effective fear-based deterrence strategy, it must exhibit the political will to take offensive action against countries like China, Russia, and North Korea, knowing they have the capability to retaliate with destructive cyber-attacks against critical infrastructure.[33] The 2015 DoD

Cyber Strategy provides few details about how the military will conduct joint operations in a contested cyber and space environment. It also does not identify what constitutes an act of war or use of force in cyberspace. Instead, the document suggests the U.S. develop more specific rules of engagement and clarify that the U.S. need not respond to a cyber-attack in kind but may use a proportional measure of traditional force instead. “The framework was drafted out of concerns that deciding when to fire in cyberspace can be more complicated than on traditional battlefield as conditions constantly shift in cyberspace, and the targets can include computer servers in different countries, including friendly ones.”[34]

Cyber weapons are unpredictable, immediate, and non-discriminating in their effects.[35] Furthermore, there is a significant risk in misattribution. If the U.S. retaliated against an innocent country, it would be viewed as an act of aggression versus an act of retaliation, as intended.[36] There is also the factor of proportionality and susceptibility when it comes to retaliation. When employing cyber-weapons, the U.S. must ensure proportionality, avoid inflicting undue collateral damage, and minimize civilian casualties.[37] In addition, countries vary in their susceptibility to reprisals in cyberspace. North Korea is a good example of this. Due to its economic primitiveness and paranoia about the outside, computers and connectivity are far less important to the national well-being of its citizens than a country like China.[38]

It is important to note that a war that starts out in the cyber domain can quickly migrate to other domains. Using cyber capabilities in unattributed, covert, grey-zone attacks increases the risk of escalation and miscalculation. Therefore, it is critical that the U.S. fully consider the second and third order effects of any pre-emptive or

retaliatory action in cyberspace, as a country's ability to mitigate events will play a significant role in determining how it will react. For example, a cyber event that might not be particularly devastating to the U.S., because of its advanced mitigation capabilities, may be permanently crippling to a less capable adversary, and subsequently result in escalation of the conflict in all domains. Conversely, despite the advanced mitigation capabilities, U.S. reliance on information networks places it at the top of the most vulnerable countries to cyber events.

Enforcement

Cyber capabilities are developing faster than the policies and doctrine to control them. While NATO-CCOE is working to develop international norms and laws regulating the cyber domain in its Tallinn Manual on the International Law Applicable to Cyber Warfare, it does not include provisions for enforcement.[39] There seems to be a desire for norms and redlines in cyberspace, but what they might be, how they will be established, and how broadly they will be accepted are still open-ended questions.[40] "There is a perverse danger to not acting in response to malicious cyber activity. Although it may be hard to deter states and non-state actors from many forms of

Current/Future Cyber Trends
State-sponsored use of hacktivist/proxies
Possible increase in self-attribution
ICS/SCADA system malfunctions
Civilian populations directly impacted
Cloud computing theft
Mobile device hacking
Internet of Things (IoT) exploitation

Figure 2. Current and Future Trends[41]

malicious cyberspace activity, it is imperative that the United States respond to such activity."[42]

Current & Future Cyber Trends

To determine an appropriate cyber deterrence strategy, it is important to examine the current trends and predict future trends to help prioritize the required elements for deterrence. A majority of the current cyber trends suggest bolstering defense, detection, attribution, and threat intelligence capabilities. See Figure 2. However, the cyber trends that have the greatest impact on the civilian population will likely require more offensive capabilities and the political will to use them.

State-sponsored cyber actors will likely continue to use independent hacktivist, proxies, and cyber criminals as cover for operations which will further test U.S. attribution and threat intelligence capabilities.43 Even if attribution can be made to a proxy, investigations must go one step further to examine possible links to state-sponsored organizations. Additionally, state-sponsored actors will likely increase their use of common nuisance malware such as ransomware to gain access to systems. This seemingly non-threatening approach makes the cyber operation appear to be a financially motivated cybercrime rather than a precursor to war. However, the ransomware may include other malicious capabilities that may go unnoticed if computer forensic experts are not actively looking for them.[44] Furthermore, malware that targets the masses makes it easier for adversaries to hide their true targets and complicate threat intelligence analysis. Use of proxies will hinder and complicate the ability of U.S. cyber forces to deter by fear.

There is some speculation that cyber actors may begin taking responsibility for cyber events to demonstrate capability and establish credibility. This is one way the

U.S. can deter adversaries through fear. However, this will not negate the need for robust attribution as the most damaging cyber events will likely remain covert. Secrecy after all, is integral to the whole concept, in that a cyberattack is only useful if the target is unaware of adversary capabilities because they are easy to defend against.[45] "Attribution will be good until it becomes useful at which point it will cease being good."[46]

Increasing "malfunctions" or "accidents" in Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) systems in the medical, water, energy, and financial sectors, directly impacting civilian populations through service disruptions, are expected. As a result, the U.S. requires increased defense and detection capabilities in these critical sectors. In 2015, Russia executed the first known successful cyberattack on a power grid, causing the information systems of three energy distribution companies in Ukraine to suspend electricity supply to consumers.[47] An exposed cyber event of this nature would likely prompt the civilian population and the government to demand significant actions such as establishing norms, redlines, laws, enforcement, and possibly retaliation.

The U.S. civilian population will likely experience an increase in targeted social engineering and misinformation campaigns designed to create an environment of confusion and distrust. Adversaries are becoming increasingly aware of the power of misinformation and how readily the public accepts the messaging. As a result, fake news sites designed to deliver scare tactics and exaggerated stories are fueling distrust among the population and causing stock market crashes.[48]

Cloud computing introduces significant new avenues of attack that can directly impact the U.S. population, requiring significant investments in defense, detection, and

threat intelligence. The data breach at Target resulted in the loss of personal and credit card information of up to 110 million individuals. “It was one of a series of startling thefts that took place during the normal processing and storage of data.”[49] Clouds contain concentrations of corporate applications and data that are susceptible to compromise if the databases are not designed properly. "If a cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well.”[50] Although, cyber breeches of this nature affect U.S. consumers and result in costly mitigations, cyber security measures rest with individual U.S. companies and the standards to which networks are protected vary. In some rare cases, commercial U.S. companies request government assistance in mitigating threats, but it is not the norm. As a result, there are no government-imposed minimum cyber security standards commercial companies must follow too receive government assistance for mitigating threats.

Criminal and state-sponsored cyber actors will likely expand capabilities against smart phones and smart devices to achieve operational objectives. According to Nokia’s Threat Intelligence Report, mobile malware infections increased 400 percent from 2016 to 2017. Android phones are reportedly the most vulnerable phones, representing 81 percent of malware infections in the second half of 2016, while iPhones and other mobile devices made up only 4 percent of attack victims.[51] As the use and functionality of smartphones increase, especially mobile financial transactions, they become a more attractive target for cyber actors. In addition, smart TVs, homes, and businesses bring about new concerns over the Internet of Things (IoT) and its susceptibility to cyber hacking. According to The Gartner, 8.4 billion connected things were in use worldwide

in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020, with each connected device serving as a potential access point for malicious cyber actors.[52] Components such as smart meters used in manufacturing field devices and process sensors for electrical generating plants connected are viable targets for any cyber adversary wishing to inflict a temporary disruption of essential services.

Current U.S. Policy on Cyber

The current U.S. policy on cyber focuses on making it difficult for intruders to gain access and establish a presence in critical networks. However, the sheer size and inter-connectedness of most critical networks makes them nearly impossible to defend. As a result, a cyber deterrence by denial policy emphasizing defense will likely fall short of achieving its objectives. Large networks with redundant, decentralized hardware and thousands of users provide more points for malicious cyber actors to gain access.[53] Despite this, the two key policy documents that guide how the Department of Defense (DoD) will implement its cyber deterrence strategies, the 2017 National Security Strategy (NSS) and the 2018 National Defense Strategy (NDS) emphasize deterrence by denial as the preferred course of action.

Pillar I of the NSS clearly states the U.S. will achieve deterrence by creating doubt in our adversaries that they can achieve their objectives. This Pillar emphasizes data protection, security and resilience of information networks, bolstering defenses, and increasing awareness of malicious activities. It does not however, rule out the possibility of offensive retaliatory measures stating a U.S. willingness to deter and disrupt cyber actors by imposing swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities.[54] The NDS also emphasizes deterrence by denial suggesting heavy

investments in cyber defense and resiliency but also recognizes the need for offensive cyber capabilities into the full spectrum of military operations.[55]

Neither the NSS nor NDS reveal a preferred deterrence approach based on target value, however it is something to consider. For example, deterrence by fear may prove as an effective strategy for critical networks such as those in the energy, financial, and nuclear sectors, whereas deterrence by denial may be a wiser approach for less critical networks.[56]

As of March 2018, a group of senators pressed President Trump to issue a national strategy for deterring malicious activity in cyberspace "as soon as possible," accusing successive administrations of not giving enough urgency to the issue. According to a letter obtained by The Hill, "The lack of decisive and clearly articulated consequences to cyberattacks against [the U.S.] has served as an open invitation to foreign adversaries and malicious cyber actors to continue attacking the United States."[57] Despite criticism that the U.S. has failed to respond to cyber events, it is likely non-public retaliations in cyberspace do occur. The benefit of maintaining this kind of strategic ambiguity is that it provides plausible deniability which may temper the possibility of escalation.

Outlook, Implications, & Recommendation

Deterrence by denial alone places the U.S. in the hopeless position of trying to discern what adversary accesses exist in its networks and how to stop such malicious intrusions.[58] On the other hand, a strategy focused on deterrence by fear increases the possibility of escalation.[59] The current U.S. policy on cyber falls short in several key elements required for a combined deterrence strategy: declared norms and redlines, credibility, and enforcement. The NSS makes it clear the U.S. has a strong interest in

protecting and defending its networks but its emphasis on denial while limiting its focus on deterrence by fear may not be a viable long-term approach.[60] According to multiple members of Congress, “A strong cyber doctrine by the United States government would serve as a deterrent, which is not only necessary, but critical to the nation’s survival in the digital age.”[61] While a cyber deterrence strategy based on fear would certainly establish the norms and redlines required for letting adversaries know which actions might prompt a retaliatory response, it could also force decision-makers into executing a potentially escalatory response option. As a result, the political will to respond to cyber events must be as strong as the desire for a cyber doctrine. One, in the absence of the other, will prove fruitless in terms of deterrence. A holistic understanding of the implications of a fear-based approach is critical, including the possibility of rapid cyber weaponization, miscalculation, and escalation. Additionally, decision-makers must be fully aware that establishing a U.S. cyber doctrine might place limitations on its own cyber operations, particularly with respect to U.S. cyber activities in the grey zone. If adversaries observe the U.S. conducting the same activities it seeks to limit, adversaries will likely not be deterred. Furthermore, they will likely use any knowledge of U.S. activities to justify their own actions.

> Defining forbidden behavior is, in cyber conflict, often an unproductive errand as cyberspace offers adversaries so many possibilities. Neither the North Korean attack on Sony nor the Russian influencing of our elections crossed any of norms proposed, after much consideration, by Secretary of State John Kerry in 2015, nor those agreed to by the G-20 later that year. And unless the United States is willing to forego our own gray zone activities, adversaries will not be inclined to back down [62]

Regardless of the criticisms, there seems to be increasing desire to formalize a cyber deterrence strategy. However, the current approach treats all adversaries and

critical infrastructure as equals. A more realistic approach is to develop multiple tailored denial and fear-based deterrent strategies for each individual adversary, considering each's differing capabilities, intent, and resolve. Furthermore, critical infrastructure must be prioritized and defended based on its value and impact to public safety if compromised. Lastly, cyber peace and furthering it by identifying global common interests, should also be explored in concert with any deterrence strategy.[63]

Endnotes

[1] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 7, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed January 27, 2018).

[2] Thomas Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University, 1960), 11, https://books.google.com/books?hl=en&lr=&id=7RkL4Z8Yg5AC&oi=fnd&pg=PA3&dq=thomas+schelling+traditional+deterrence+theory&ots=42pX1c0Zmi&sig=3o3QNN9KR6eu6jd5YEj7HG7poD4#v=onepage&q=thomas%20schelling%20traditional%20deterrence%20theory&f=false (accessed February 5, 2018).

[3] A. Wess Mitchell, "The Case for Deterrence by Denial," *The American Interest*, August 12, 2015, https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/ (accessed February 5, 2018).

[4] T.V. Paul, Patrick M. Morgan, and James J. Wirtz, *Complex Deterrence: Strategy in the Global Age*, (Chicago, IL: University of Chicago Press, 2009), 55, https://books.google.com/books?id=oZOsiAlOEiQC&pg=PA55&dq=DO-JOC+restraint&hl=en&sa=X&ved=0ahUKEwiry7aamIXaAhWEtlkKHRQOBwEQ6AEIJzAA#v=onepage&q=DO-JOC%20restraint&f=false (accessed March 24, 2018).

[5] Thomas Schelling, *The Strategy of Conflict*, 11.

[6] Mitchell, "The Case for Deterrence by Denial."

[7] Bernard Brodie, *The Anatomy of Deterrence in Strategy in the Missile Age* (Princeton, NJ: Princeton University Press, 1959), 264–304.

[8] AtomicArchive.com, "Cold War: A Brief History on Nuclear Deterrence," 2015, http://www.atomicarchive.com/History/coldwar/page15.shtml (accessed February 9, 2018).

[9] Gray zone operations are characterized by ambiguity, exploitation of weaknesses using all elements of national power, attacks in multiple domains, use of criminal organizations and networks, and using laws and cultural norms to achieve an advantage. Enemies exploit the

inherent advantages in these characteristics to achieve their strategic objectives while staying below the threshold of full-scale conflict.

[10] Mitchell, "The Case for Deterrence by Denial."

[11] Jim Garamone, "Dunford Details Implications of Today's Threats on Tomorrow's Strategy," August 23, 2016, linked from *DoD News, Defense Media Activity,* https://www.defense.gov/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy/ (accessed March 24, 2018).

[12] Tom Olzak, "Cyberwarfare: Characteristics and challenges," *TechRepublic* blog entry posted June 24, 2013, https://www.techrepublic.com/blog/it-security/cyberwarfare-characteristics-and-challenges/ (accessed March 24, 2018).

[13] Timothy McKenzie, *Is Cyber Deterrence Possible?* (Maxwell AFB, AL: Air University Press, January 2017), 21, https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF (accessed March 12, 2018).

[14] Kelsey Atherton, "Chinese Hackers Steal Plans To Dozens Of U.S. Weapons Systems," *Popular Science*, May 28, 2013, https://www.popsci.com/technology/article/2013-05/cyber-spies-compromise-over-two-dozen-weapons-systems (accessed March 24, 2018).

[15] Adam Howard, "Obama White House Stands by Free Speech in Sony Hacking Scandal," *MSNBC*, December 18, 2014, http://www.msnbc.com/msnbc/obama-white-house-stands-free-speech-sony-hacking-fight (accessed March 24, 2018).

[16] Tory Newmeyer, "Obama to China: Stop hacking U.S. companies, or else," *Fortune*, September 16, 2015, http://fortune.com/2015/09/16/obama-warns-china-on-hacking/ (accessed March 24, 2018).

[17] Dr. Martin C. Libicki, "It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture," Testimony before the House Committee on Armed Services, *Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities*, March 1, 2017, 6, http://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Wstate-LibickiM-20170301.pdf (accessed March 10, 2018).

[18] James Van de Velde, "How Deterrence Fundamentals Function in Cyberspace," *The Cipher Brief*, October 6, 2017, https://www.thecipherbrief.com/column_article/deterrence-fundamentals-function-cyberspace (accessed December 26, 2017).

[19] Aidan Quigley, "Obama Ordered "Cyberbombs' in Response to Russian Hacking: Report," *Newsweek*, June 23, 2017, http://www.newsweek.com/obama-ordered-cyber-bombs-response-russian-hacking-report-628597 (accessed January 19, 2018).

[20] Dawn A. Hicks, *Policy Analysis: Russian Cyber Deterrence*, Regional Studies Paper (Carlisle Barracks, PA: U.S. Army War College, January 10, 2018).

[21] Greg Miller, Ellen Nakashima, and Adam Entous, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," *The Washington Post,* June 23, 2017.

[22] Figure created by the Author.

[23] Vincent Scotti Jr, *Computer Network Security: The Challenges of Securing a Computer Network*, (Cocoa, FL: Brevard Community College, 2011), 8, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110014451.pdf (accessed February 9, 2018).

[24] Michael Ruhle, "Deterrence: what it can (and cannot) do", *NATO Review Magazine*, 2015, https://www.nato.int/docu/review/2015/Also-in-2015/deterrence-russia-military/EN/index.htm (accessed February 9, 2018).

[25] Libicki, "It Takes More than Offensive Capability," 5.

[26] Mandiant, *M-Trends 2014 Annual Threat Report: Beyond the Breach* (Milpitas, CA: FireEye, 2014), 1, https://www2.fireeye.com/fireeye-mandiant-m-trends-report (accessed March 9, 2018).

[27] Verizon, *2014 Data Breach Investigations Report* (New York, NY: Verizon Communications Inc., 2014), 53, http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf (accessed March 9, 2018).

[28] HPE Enterprise Security Team, "Introduction To Cybersecurity Threat Detection Analytics", *TechBeacon*, https://learn.techbeacon.com/units/introduction-cyber-security-threat-detection-analytics (accessed March 9, 2017).

[29] A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

[30] Mandiant, *M-TRENDS: A View From the Front Lines 2017* (Milpitas, CA: FireEye, 2017), 2017, 1, https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html (accessed March 9, 2017).

[31] Ibid.

[32] Keith B. Alexander, "Prepared Statement on Cyber Strategy and Policy," Testimony before the Senate Armed Services Committee, March 2, 2017, 3, https://www.armed-services.senate.gov/imo/media/doc/Alexander_03-02-17.pdf (accessed March 10, 2018).

[33] Thomas C. Schelling, *The Diplomacy of Violence* (New Haven, CT: Yale University Press, 1966), 1-34.

[34] Ellen Nakashima, "List of Cyber-Weapons Developed By Pentagon To Streamline Computer Warfare", March 31, 2011, *The Washington Post*, May 31, 2011, https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html?utm_term=.13e52ff2e32b (accessed December 26, 2017).

[35] CyberWire, "Cyber Deterrence: Attribution and Ambiguity (and Certainty, too)," 2016, https://thecyberwire.com/events/inss2016/intelligence-and-national-security-summit-2016-cyber-deterrence-attribution-and-ambiguity.html#sthash.f5fUx0oW.dpuf (accessed March 12, 2018).

[36] Libicki, "It Takes More than Offensive Capability," 7.

[37] Nakashima, “List of cyber-weapons.”

[38] Libicki, “It Takes More than Offensive Capability,” 2.

[39] Adam Segal, “Can Finland Act As a Mediator on Cyber Norms?” *Council on Foreign Relations* blog entry posted May 28, 2015, https://www.cfr.org/blog/can-finland-act-mediator-cyber-norms (accessed 10 March 2018).

[40] Jarno Limnel, “The Reality of Cyberwar: Current Concepts and Future Trends,” *European Cybersecurity Journal* 1, no. 2, (2015): 40, https://cybersecforum.eu/files/2016/12/ecj_vol1_issue1_j.limnel_the_reality_of_cyberwar_current_concept_and_future_trends.pdf (accessed March 9, 2018).

[41] Figure created by the Author.

[42] Van de Velde, “How Deterrence Fundamentals Function in Cyberspace.”

[43] Jack Detsch, “How Russia and Others Use Cybercriminals As Proxies,” *The Christian Science Monitor*, June 28, 2017, https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies (accessed March 10, 2018).

[44] Andy Greenberg, “Petya Ransomware Epidemic May Be Spillover From Cyberwar,” *Wired*, June 28, 2017, https://www.wired.com/story/petya-ransomware-ukraine/ (accessed March 10, 2018).

[45] Danny Vinik, “America’s Secret Arsenal,” *The Agenda*, December 9, 2015, https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331 (accessed March 10, 2018).

[46] Libicki, “It Takes More than Offensive Capability,” 3.

[47] Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid,” *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, (accessed January, 29, 2018).

[48] Tim O'Neill, “Fake News Is More than Just Misinformation—What to Do About Malvertising,” *TAP Into Technology* blog entry posted December 13, 2016, https://www.garlandtechnology.com/blog/fake-news-is-more-than-just-misinformation-what-to-do-about-malvertising (accessed March 10, 2018).

[49] Charles Babcock, “9 Worst Cloud Security Threats,” *InformationWeek*, March 3, 2014, https://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085 (accessed March 11, 2018).

[50] Bob Violino, “The Dirty Dozen: 12 Top Cloud Security Threats For 2018,” *CSO Online*, January 5, 2018, https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html (accessed March 11, 2018).

[51] Nokia, *Nokia Threat Intelligence Report—2017*, (Espoo, Finland: Nokia, 2017), 6, https://onestore.nokia.com/asset/201621/Nokia_2017_Threat_Intelligence_Report_EN.pdf (accessed March 11, 2018).

[52] Rob van der Meulen, “Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016”, *Gartner*, February 7, 2017, https://www.gartner.com/newsroom/id/3598917 (accessed March 11, 2018).

[53] IT Direct, “The Top 3 Issues Affecting Today’s Large Computer Networks,” *IT Direct* blog entry posted February 1, 2012, https://www.gettingyouconnected.com/the-top-3-issues-affecting-todays-large-computer-networks/ (accessed February 9, 2018).

[54] Donald J. Trump, *National Security Strategy* (Washington, DC: The White House, February 6, 2015), 13, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed January 22, 2018).

[55] Department of Defense, *The National Defense Strategy of the United States of America 2018* (Washington, DC: U.S. Department of Defense, January 2018), 6, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed January 27, 2018).

[56] Benjamin Edwards et al., “Strategic Aspects Of Cyberattack, Attribution, And Blame,” *PNAS*, March 14, 2017, http://www.pnas.org/content/114/11/2825 (accessed February 12, 2018).

[57] Morgan Chalfant, “Senators Demand Cyber Deterrence Strategy From Trump,” *The Hill*, March 3, 2018, http://thehill.com/policy/cybersecurity/377410-lawmakers-demand-cyber-deterrence-strategy-from-trump (accessed March 11, 2018).

[58] Van de Velde, “How Deterrence Fundamentals Function in Cyberspace.”

[59] Ibid.

[60] McKenzie, *Is Cyber Deterrence Possible?*,5.

[61] Chalfant, “Senators Demand Cyber Deterrence Strategy.”

[62] U.S. Congress, House of Representatives, Committee on Armed Services, *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities,* 115th Cong., 2nd sess., March 1, 2017, 4, https://financialservices.house.gov/uploadedfiles/hhrg-114-ba15-wstate-jhealey-20150519.pdf (accessed March 11, 2018).

[63] Limnel, “The Reality of Cyberwar,” 45.