8-1-2013

Robustness: A New US Cyber Deterrence Strategy

Eric M. DeCampos
University of Denver

Robustness: A New U.S. Cyber Deterrence Strategy

_____

A Thesis

Presented to

the Faculty of the Josef Korbel School of International Studies

University of Denver

_____

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

_____

By

Eric M. DeCampos

August 2013

Advisor: Dr. Paul R. Viotti

Author: Eric M. DeCampos
Title: Robustness: A New U.S. Cyber Deterrence Strategy
Advisor: Dr. Paul R. Viotti
Degree Date: August 2013

Abstract

The growing trend of computer network attacks provokes the necessity for a comprehensive cyber deterrence strategy to deter aggressors from attacking U.S. critical infrastructure. The current U.S. cyber deterrence strategy based on punishment is ineffective in deterring aggressors as evidenced by the increasing number of computer network attacks against U.S. critical infrastructure. Therefore, the U.S. should look towards an alternative strategy based on robustness to deny enemy objectives and absorb attacks. To identify the superior cyber deterrence strategy, this study uses a qualitative assessment based on open-sourced information to evaluate the effectiveness of each strategy. The findings of this study show that a deterrence strategy centered on robustness can be more effective in deterring aggressors. As a result, the United States would be better served to reform its cyber deterrence strategy by establishing a capability to absorb computer network attacks and deny enemy objectives as a deterrent.

Acknowledgments

I wish to thank various people for their contribution to this project; Dr. Szyliowicz and Dr. Viotti, for their valuable assistance in developing this master's thesis; Dr. Lewis Griffith, for his invaluable insight and constructive recommendations. Special thanks are given to Mr. Brent Shapiro and Dr. Benjamin Gochman for their professional guidance and valuable support. Finally, I wish to thank all those who have supported and encouraged me throughout this project.

Table of Contents

Chapter 1: Introduction

The United States (U.S.) has been consistently victimized by computer network attack (CNAs) from state and non-state actors, with the annual number of CNAs against U.S. critical infrastructure having increased seventeen-fold since 2009.[1] The current state of the debate on how serious the threat posed by such attacks is and what to do about it is divided between alarmists and cynics. Alarmists, such as former U.S. Secretary of Defense Leon Panetta, advocate that the growing trend of CNAs against the United States increases the likelihood for a strategically placed CNA to generate the equivalent of a cyber Pearl Harbor. While clearly not a direct parallel, a cyber Pearl Harbor is used as an analogy for the catastrophic damage and disruption to daily life that can arise when a CNA is used to destabilize critical infrastructure. While speaking at the Intrepid Sea, Air, and Space Museum in New York, Panetta described the increasing technological aggressiveness of states, like China, and non-state actors, such as the now famous hactivist collective known as Anonymous, can derail critical infrastructure in the United States.[2] For example, Mandiant, a private cybersecurity firm, has recently attributed a new wave of CNAs against private firms directly connected to the U.S. electric grid to

[1] Sanger, David E., and Eric Schmitt. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." The New York Times, July 26, 2012. http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=0.

[2] Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S."*The New York Times*, October 11, 2012. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

Chinese state-sponsored hackers. Other policymakers, such as U.S. Representative Trent Franks, have echoed Panetta's rhetoric, warning "*If we don't change our course, national electric grids could be headed for disaster."*[3] To prevent such a catastrophic occurrence, alarmists have argued one key option to decrease the likelihood of a cyber Pearl Harbor is to strike or retaliate against the aggressor.[4]

Cynics, like cryptologist Bruce Schneier, refute this analogy as an exaggeration used for political gain or funding. Although the potential consequences of a CNA on U.S. critical infrastructure can be severe, cynics argue that such an event does not pose an existential threat to the United States. However, such consequences are possible and mitigating them must be accounted for. Cynics advocate that preventing these consequences by threatening force against possible aggressors is not the answer. Schneier argues that the U.S. should focus on cyber defense and bolster the resiliency of its critical infrastructure as an alternative to using force. Nevertheless, alarmists have come to dominate the policy debate. Their solution of choice is cyber deterrence, coercing aggressive actors from attacking the state via cyberspace, whether in the form of a CNA or otherwise, through threats of pre-emptive action and retaliation. [5]

---

[3] Burgess, James. "Chinese Military Renews Cyber-Attacks, Focusing on US Electrical Grid." Oil Prices & Energy News: Crude Oil Price Charts, Investment Advice. Last modified May 23, 2013. http://oilprice.com/Latest-Energy-News/World-News/Chinese-Military-Renews-Cyber-Attacks-Focusing-on-US-Electrical-Grid.html.

[4] Bumiller and Shanker. "Panetta warns of dire threat of cyberattack on u.s." *The New York Times.*

[5] Armending, Taylor. "Security Experts Push Back at 'Cyber Pearl Harbor' Warning." CSO. Last modified November 7, 2012. http://www.csoonline.com/article/720930/security-experts-push-back-at-cyber-pearl-harbor-warning.

Alarmists within policymaking circles have, as their fundamental understanding of cyber deterrence, a Cold War perspective. These policymakers subscribe to deterring aggressive actors by threatening force against the aggressor or their valued interests. Such tactics are comparable to U.S. deterrence strategies formulated against the Soviet Union during the Cold War and through which the U.S. threatened to utilize its nuclear arsenal against the Soviet Union should it attack the homeland, its allies, or its vital interests. Similarly, the present U.S. cyber deterrence strategy (USCDS) threatens to preemptively strike or respond against aggressors should they attack U.S. critical infrastructure through cyberspace. In reality, the United States has yet to achieve the same success in deterring enemies in cyberspace as it did deterring the Soviet Union during the Cold War, evidenced by the consistency of CNAs against U.S. critical infrastructure. This reality lends credence to the notion that current USCDS based on Cold War strategies is ineffective in deterring America's enemies.

There is a fundamental and contextual difference between the current USCDS and the Cold War tradition model that explains the failure of U.S. cyber deterrence. During the Cold War, the United States prevented an enemy that had not acted, and it turns out, was already deterred, at least following the establishment of mutual nuclear arsenals. Deterrence strategies during the Cold War were not designed to prevent an enemy already striking at U.S. interests, a far more daunting task. Unlike its conflict with the Soviet Union, the United States is faced with enemies who have already and continue to attack via cyberspace. This fundamental difference fosters the need to first re-establish

and then maintain deterrence against reoccurring attacks. The current USCDS fails to address these necessities given the increasing number of CNAs against the United States.

Thus, deterrence under the Cold War perspective is not the answer. The realities of the present cyber environment, such as the inability to prevent all threats posed to the BES or the evolving offensive cyber capabilities of U.S. rivals, demonstrates the necessity for a different approach to cyber deterrence. I believe a USCDS based on robustness, where critical infrastructure is able to absorb CNAs while ensuring continuity of service and denying the enemy's objectives, can address these realities. Traditionally, deterrence is achieved by persuading aggressive actors, whether with the threat of force or by denying their objectives, from attacking the state and to maintain their deterred behavior. For the purposes of this discussion, I assert that the same should be true for a USCDS based on robustness as the U.S. can threaten to deny enemy objectives by absorbing CNAs, persuade aggressors from attacking via cyberspace, and then maintain their deterred behavior, in the future.

Prior to delving further into the issue, there is a fundamental empirical concern that must be addressed. Like other national security issues that are highly government-centric, such as terrorism for example, significant and relevant information regarding both attacks and steps taken in response to CNA efforts against the U.S. government are unavailable to this research effort. For example, not included here is comprehensive information from the National Security Agency (NSA) or the U.S. Cyber Command (USCYBERCOM), both of which are leading federal agencies in any effort at cyber-defense. Thus, due to access and classification issues, there is no way to build a

quantitative assessment of the current effectiveness of the USCDS or any alternative approaches based on anything approaching a population or even highly reliable sampling frame of real world data. To avoid the potential internal and external validity issues that would come from any effort to sample from the available data without a real understanding of the population as a whole, this study analyzes only open-sourced information be it from the Executive Office of the President, the Department of Homeland Security, corporate security sources, and academic and other research.

This information was used to specifically assess whether the current USCDS is more effective in deterring aggressors than an alternative USCDS based on robustness via a qualitative assessment to identify the superior USCDS. The assessment evaluates the effectiveness of each USCDS by comparing their capabilities to address eight specific criteria that any meaningful cyber-defense effort would desire to maximize: the attribution problem, scalability, contestability, the regulation problem, the Spy-VS-Treaty problem, socio-political costs, and economic costs. In this way, it is possible to logically evaluate how effective the current cyber-deterrence approach advocated by the Obama Administration's USCDS is in addressing the current array of known threats, construct an alternative approach that maximizes the ability to provide meaningful cyber-defense in the form of robustness, and then compare, using these common criteria, the two approaches following laying out how robustness would apply to the Bulk Electrical System (BES) as a single, demonstrating case study. Based on the results of the qualitative assessment, I am able to claim that an alternative USCDS based on robustness is more effective in deterring aggressors and minimizing the threat posed by CNAs than

the Obama Administration's USCDS. This means that the United States government must re-evaluate its national strategy towards cyber deterrence and the protection of its critical infrastructure. If the alternative USCDS based on robustness is implemented, the U.S. government should also take measures to mitigate the limitations of its future USCDS to maximize the strategy's effectiveness.

The thesis executes this analysis in the following manner. Chapter Two, explores, from an historical standpoint, the nature of the threat posed by cyber-attackers, the debate surrounding cyber deterrence during the 1990s, and how the Cold War philosophy towards deterrence has shaped alarmist policymakers' development of a cyber deterrence strategy based on punishment. Then, it will be possible to analyze current White House policies on cyber deterrence, such as the *International Strategy for Cyberspace*, to illustrate their limitations and ineffectiveness on deterring aggressors. Chapter Three proposes an alternative USCDS based on robustness designed to deny enemy objectives. My proposed strategy is framed with the analysis of Robert Art and Robert Pape's work to determine whether denial deterrence, when the aggressor is undermined to the point where it begins to doubt its own strategy and thus does not engage in hostilities, is viable in cyberspace.[6] Upon concluding that denial deterrence is indeed viable, I then discuss the necessary criteria, identified by cybersecurity scholars such as Richard Andres and Jeffrey Cooper, which a successful cyber deterrence strategy must address and overcome. Chapter Four applies my proposed USCDS to the Bulk Electric System (BES) through examples of defensive postures and redundancy, as well the ability to tailor a response

[6] Pape, Robert A. *Bombing to Win: Air Power and Coercion in War*, 4-6. Ithaca, N.Y.: Cornell University Press, 1996.

against a CNA. Chapter Five presents a qualitative analysis to assess which USCDS, my proposed strategy based on robustness or the current strategy based on punishment, is more effective in deterring cyber-attackers. I use information collected from secondary sources, such as the RAND Corporation and the Executive Office of the President, to identify whether each USCDS can address eight criteria affecting cyber deterrence.

I conclude in Chapter Six with a discussion of my findings drawn from the qualitative analysis presented in the previous chapter. The assessment shows that the alternative USCDS based on robustness can be more effective than the current strategy. This is due to the fact that it mitigates most of the factors limiting cyber deterrence as opposed to the current USCDS; thus, the proposed alternative strategy has a potential for greater success in deterring aggressors from attacking critical infrastructure via cyberspace. However, there are some factors limiting the alternative USCDS in the wake of sequestration in the United States and a polarized Congress. As a result, I also develop three recommendations to mitigate the limitations of the alternative USCDS and increase its viability.

Chapter 2: U.S. Cyber Deterrence; A Review

The dynamic nature of cyberspace has frustrated policymakers in their attempt to preserve U.S. national security and protect assets in an environment as dynamic as cyberspace. Cyber security is a muddled subject as the United States continues to counter attacks from both state and non-state attackers. If one cannot keep up with elusive aggressors that continue to come up with new ways to conduct cyber-attackers against the United States, then the simplest way to address this issue is to make the costs of such an attack greater than its benefits. Chapter 2 will review the nature of cybersecurity, the history of American cyber deterrence, and discuss the current official cyber strategy.

Realities of Cybersecurity

One reality hindering cyber security frameworks is the reality that cyber-defense capabilities do not evolve at the same rate as offensive capabilities. The speed by which malware, viruses, and other malicious programs evolve cannot be matched by the preventative measures developed by government agencies and the private sector. For example, the 2010 discovery of the Stuxnet virus came with the realization that the program had gone undetected for months. The virus targeted energy installations across the world and was only discovered after damage had been incurred. One reason behind the sluggish evolution of cyber defenses is the inadequate number of qualified personnel to create and administer cyber security protocols for critical infrastructure. Using the Bulk Electric System as an example, the movement towards implementing Smart Grids in

the United States will require two to three times more professional technicians to administer North America's electric grids and secure them from potential threats. As critical infrastructure becomes more integrated and interconnected, their vulnerabilities will drastically increase due to the lack of trained professionals with the knowledge and understanding of delivery systems security risks. Given the dynamic nature of offensive cyber capabilities, it is only a matter of time before current prevention strategies become obsolete. [7]

This leads to the next reality inhibiting cyber-defense frameworks; the United States is unable to prevent every single cyber-attack against it. Based on the notion that defensive capabilities evolve at a slower rate, it is highly improbable that the U.S. can identify and destroy all digital threats to its critical infrastructure. This is evident by the consistent intrusions against U.S. cyberspace by malicious cyber-attackers. Only after this key assumption has been accepted can the development of successful strategy for cyber-defense be developed. In summary, both realities obstruct the effectiveness of U.S. cyber deterrence as malicious hackers have an offensive advantage that emboldens rather than deters aggressors. The United States must look towards other means and strategies to be able to counter cyber-attacks; even if these attacks can't be prevented.[8]

---

[7] U.S. Department of Energy and the North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System: A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop*. 2010. Accessed February 17, 2013. http://www.nerc.com/files/HILF.pdf.

[8] Ibid.

Cyber Capabilities and Threats

Although there are a number of obstacles that can inhibit a target's cyber deterrence framework, the ultimate threat is the attacker and its capabilities. There are two forms of capabilities that characterize a cyber-attack; man-made deliberate threats and untargeted attacks. A man-made deliberate attack (MMDA) is defined as the use of malicious capabilities to attack a specific system or network of critical infrastructure by a state, group, or individual (e.g., disgruntled employees, states, criminal syndicates, or hackers). An example of this form of attack includes the use of a vector, such as a worm, virus, or other malicious software, to target a specific system from a designated target. Conversely, an untargeted attack (UA) occurs when the target of an attack is undefined. These attacks often employ the same vectors as a MMDA despite the lack of a target, such as the release of malicious software onto the internet in order to create a botnet. Both attacks will utilize the same vectors for attack with the sole difference being the intent. Vectors include denial of service attacks, reconnaissance attacks, unauthorized access attacks, and collateral damage.[9]

Distributed Denial of Service Attacks

One of the most effective weapons at a cyber-terrorist's disposal is a distributed denial of service (DDoS) attack. This capability targets the communication protocols of a server in order to disrupt the operational commands being distributed within the server. [10]

---

[9] U.S. Department of Energy. *Roadmap To Achieve Energy Delivery Systems Cybersecurity*. 2011. Accessed May 20, 2013. http://energy.gov/sites/prod/files/Energy Delivery Systems Cybersecurity Roadmap_finalweb.pdf.

[10] U.S. Department of Energy and the North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*.

The strategy behind this attack is to flood the server with an astronomical number of commands to the point where the server is either unable to process the flood or requests or its operating speed is lowered.[11] This form of attack is a man-made deliberate attack. DDoS attacks are not a new phenomenon but have recently garnered world-wide attention because of its use by cyber-terrorist groups such as Anonymous. Anonymous has utilized DDoS attacks to disrupt services rendered by corporate goliaths such as Mastercard and PayPal. U.S. government servers are also at risk from DDoS attacks, as illustrated by attacks attributed to Anonymous on the U.S. Department of Justice, the Copyright Office, and the U.S. Central Intelligence Agency homepage.[12] Although many of these attributed DDoS attacks have targeted U.S. government and corporate entities, there is nothing prohibiting the use of this low technology but highly effective capability to target critical infrastructure in the United States.

Reconnaissance and Eavesdropping Attacks

Not all attacks are designed to disrupt company services, or in the case of the electric grid, disrupt the flow of electricity. Cyber-terrorists are just as keen to collect information on their targets as they are to maim or destroy them. To successfully engage in this form of cyber-espionage, cyber-terrorists will use reconnaissance attacks to gather information on public entities or private citizens. Reconnaissance attacks collect information on the vulnerabilities of critical infrastructure. Cyber-attackers spend a significant amount of time observing their target's defense mechanisms and how

[11] Ibid.

[12] Albanesius, Chloe. "Anonymous Takes Down CIA Web Site." PCMAG. Last modified February 10, 2012. http://www.pcmag.com/article2/0,2817,2400140,00.asp.

information is transmitted. For example, they will determine the strength of the target's firewall or the type of systems that they are using to manage their cyber defenses. In the case of public utilities, cyber-attackers will assess the security of the target's infrastructure and the level of security guarding confidential customer information pertaining to customers. Once information has been obtained regarding the target's network information, host information, security policies, and personnel or customer information, cyber-terrorists can pinpoint the exact vulnerabilities of their target and tailor their attacks accordingly.[13]

There are two forms of reconnaissance attacks at the disposal of cyber-attackers. First, passive reconnaissance employs covert means of infiltration and espionage with the goal of this leaving minimal evidence or traces showing an infiltration of a server. The best example of passive reconnaissance is illustrated by the recent discovery of the Flame virus by a Russian information technology security firm. Operating across the world since 2010, Flame is a malware program designed to attack computers run by the Microsoft Windows operating system. Flame is designed to record audio, screenshots, keyboard activity, and network traffic. The program has been known to record Skype, a global online communication service, conversations. The malware spreads from computer to computer through a computer's Bluetooth function, spreading to other systems that contained the wireless data exchange program. Once data on the targeted system has been collected, the malware is designed to transmit the data to designated command servers scattered across the world and await further instructions. This program

[13] U.S. Department of Energy and the North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*.

has been dubbed the most sophisticated and most complex malware ever found; leading experts to suspect it was created by a state actor for the purpose of espionage. The second form of reconnaissance attacks are active attacks. This form is characterized by overtly attempting to collect information without discretion. Such an overt strategy can be accomplished through intrusive means such as scanning. Scanning is used by cyber-terrorists to every port number of a specific Internet Protocol (IP) address to determine which ports are open and in operational use. This measure is intrusive because the target can be alerted to the scan and it results in strange connections to the target's server.[14]

Collateral Damage

When cyber-attackers attempt to inflict damage upon targets, there is a strong likelihood that their attacks will have secondary impacts. Collateral damage, in cyberspace, is defined as the unplanned side-effects of cyber-attacks. This can occur in many different ways, whether planned or not. In the case of defending critical infrastructure, collateral damage may target many different entities at once, including infrastructure, civilians, or government agencies. For example, a cyber-attacker attempting to disrupt power in Manhattan can unintentionally spark a power surge in adjacent grids in New England. When the disruption occurs, the power surge will travel through connected transmission lines across the region resulting in loss of power in Vermont and New Hampshire. Collateral damage in this example can affect public utility workers servicing transmission lines impacted by the surge. Continuing with the example; when the blackout in Manhattan occurs, the excess energy will surge through

[14] Brown, Chris. "Phases of a Cyber-attack / Cyber-Recon." United States Naval Academy. Accessed July 17, 2013. http://www.usna.edu/CS/si110arch/si110AY12F/lec/l32/lec.html.

transmission lines being serviced by public utility workers, injuring or killing them in the process. This form of attack is untargeted, because cyber-terrorists are uncertain about the after-effects sparked by collateral damage. However, it is very likely that these cyber-attacks are planned to result in collateral damage with greater human and infrastructure casualties.[15]

Unauthorized Access Attacks

The most dangerous capability at a cyber-attacker's disposal is the use of unauthorized access attacks. This capability allows cyber-terrorists to exercise a degree of control over targeted systems to steal or manipulate data without authorization. This manipulation of assets, service, or information can result in disastrous implications, as system operators will be exposed to compromised data that can influence their decision-making calculus and negatively impact the system. In the case of the electric grid, this form of attack would target operational commands between power nodes. In this scenario, operational commands can be manipulated to generate harmful amounts of electricity that can cause power surges or other potential complications.[16]

MMDA and UAs can easily be used against critical infrastructure to cause severe socio-political and economic costs that can cripple the United States. These forms of attack can directly target critical infrastructure or use them as weapons to cause further chaos. These grim possibilities make cyber deterrence a vital necessity to protect the United States and deter enemies from striking its most vulnerable infrastructure by any of

[15] U.S. Department of Energy and the North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*.

[16] Ibid.

a number of means. To lend further credibility to this threat is the fact that precedence for targeting critical infrastructure has already been set through the use of the Stuxnet virus on Iranian energy infrastructure. Although the U.S. has officially admitted to using the Stuxnet virus, the attack did set precedence for how an attack on critical infrastructure would go about. Furthermore, the U.S. attack on Iranian infrastructure has opened the floodgates for similar attacks to be waged in the United States. The only fashion to effectively stop state and non-state actors from launching an attack similar to the Stuxnet virus in the United States is to effectively deter them.

The History of U.S. Cyber Deterrence

President Obama remarked in 2009, "the very technologies that empower us to create and to build also empower those who would disrupt and destroy."[17] Those words echo the belief that America has become so dependent upon its technology that cyber space stretches across every segment of the economy and, of course, the heart of American society. For example, the BES is among the sectors most heavily dependent upon cyberspace. The majority of SCADA (supervisory control and data acquisition) systems used by operator(s) of the Bulk Electric System (OBES) issue commands across their segment of the national grid, as they also remain linked in one way or another to anyone desiring to access the system. Through its connection to the company network that also contains access to the Internet or through remote terminal units with wireless connectivity; more devices within the electric grid are becoming interconnected with

[17] Obama, Barack H. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Executive Office of the President of the United States, 2009. Accessed March 15, 2013. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

cyberspace. This trend will continue as OBES experiment with Smart Grids and Smart Meters to increase efficiency and sustainability. This technology, as discussed in Chapter 1, has left OBES vulnerable to malicious actors who can access Smart Meters remotely through cyberspace. As such, the need for an effective cyber defense strategy is more pressing than ever, with cyber deterrence as the preferred option. Yet cyber-deterrence has been a topic for discussion for the past twenty years and predates the publicized cyber-attacks on Estonia (2007) and Georgia (2008), and was first discussed during the Gulf War in the 1990s.

Net War V. Cyber War (1990-2000)

In 1990, the Saddam Hussein's Iraq launched an offensive campaign to capture valuable oil fields from its smaller neighbor, Kuwait. The invasion of Kuwait and subsequent hostile rhetoric towards neighboring Saudi Arabia by Hussein resulted in the passage of U.N. Resolution 678 in November 1990. This UN resolution authorized the use of force to enforce UN Resolution 660, which had demanded the withdrawal of Iraqi forces from Kuwait. Operation Desert Storm and UN Resolution 660 ushered in a new era of information warfare using offensive cyber capabilities. Information warfare was used by the United States and its UN coalition partners to exploit information to compliment its conventional warfare strategy against Iraq. The Gulf War was viewed as an instance of cyber war in which information technology was operationalized by one state military against another. In contrast, net wars are different from cyber wars because they occur from societal conflicts that include non-state actors. This key distinction separating state from non-state cyber-attackers shaped early frameworks for a proposed

comprehensive cyber deterrence strategy. Policymakers and academic scholars argue that deterring a state actor was a different challenge than deterring a non-state actor.[18] State actors respond to costly signals such as strong military postures or economic sanctions. As a result, it is much easier to deter a state actor with the threat of retaliation than deter non-state actors with the same strategy.[19]

In contrast, non-state actors are more difficult to coerce due to their lack of high valued assets, their ability to cloak themselves into their environment, and the difficulty to signal them.[20] The asymmetric nature of non-state actors provides them with an advantage against organized state actors, making deterrence difficult to achieve. More importantly, a net war against a non-state actor would require the implementation of deterrence by denial designed to deny the enemy from achieving its goals, attributing the enemy, and successfully retaliating against the enemy. Moreover, scholars believe that the implementation of an objective denial strategy would only dissuade the enemy, inducing restraint and reducing its capabilities.[21] This resulted in a debate regarding the effectiveness of net war deterrence relative to the classical approach of using a strong cyber posture and costly signals to deter state actors. Some believe that deterrence was merely a by-product of a greater strategy based on the perception of retaliatory

---

[18] Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (2012): 148-170. doi:10.1080/13523260.2012.659597.

[19] Ibid.

[20] Thomas, Troy S. "Beyond Pain: Coercing Violent Non-State Actors." Last modified 2010. http://www.usafa.edu/df/inss/Research Papers/2010/Thomas Coercing VNSA.pdf.

[21] Stevens. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

capabilities.[22] However, opposing scholars believed that deterrence can be achieved through America's technical prowess to threaten what enemy's hold dear and thereby influence their decision-making calculus.[23]

From Perceptions to Attacks (2001-2008)

The new millennium ushered in a new era for cyber security as digital attacks became more sophisticated and the implications increased exponentially. The discussion among scholars and policymakers regarding creating a national deterrence strategy changed from one based on perception management to a concern with deterring computer-based attacks on critical infrastructure. Most significantly, the cyber security community began to realize the importance of countering attacks such as cyber espionage, crime and terrorism. Emphasis was then placed on preventing those types of attack from occurring and increasing protective measures in cyberspace. Thus, a formidable deterrence strategy was needed to ensure that the possibility of attack would be more deleterious than advantageous to the aggressor.[24]

On the other hand, many scholars and policymakers believed that cyber deterrence can never be achieved. According to Patrick Morgan, the previous discussions on a national deterrence framework fail to identify conditions for deterrence. First, previous strategies fail to take into consideration the rationality of attackers given the inclusion of non-state actors and the different motivations they may have relative to state

[22] Ibid.

[23] Ibid.

[24] Ibid.

actors. Second, the inclusion of non-state actors makes any form of retaliation challenging due to the difficulty of attribution. Many scholars acknowledge the challenges of attribution, but still consider deterrence through punishment as a viable option against non-state actors. Third, it was difficult to ascertain an attacker's assets to exploit with the threat of punishment. Fourth, the absence of proper rules of engagement as agreed upon by the international community creates an issue of scalability and increases the risk of losing international social capital should the United States fail to respond appropriately. Fifth, little stability in response makes the chances of a physical conflict between the attacker and the target more likely. The sixth and final point as to why cyber deterrence is unattainable, according to Morgan, is the notion that there exists no such severe conflict in the military sense, making retaliation difficult to legally justify.[25]

Morgan's opinion of cyber deterrence was derived from the application of nuclear deterrence strategies to cyberspace. Cyberspace is more complex and dynamic than the mutually assured destruction that made nuclear deterrence possible during the Cold War. Retaliating against an enemy in cyberspace is still possible, but is it the preferred strategy? As cyber-attacks on the U.S. and its allies continued to rise, scholars debated whether cyber deterrence should focus on the concept of mitigation attacks and objective denial, or take a Cold War perspective through punitive deterrence. A breakthrough ultimately emerged in the academic work of Richard Harknett and his views on denial deterrence. Harknett debated whether denial could even be considered a form of

[25] Morgan, Patrick M. *Deterrence Now*, 8. Cambridge [England]: Cambridge University Press, 2003.

deterrence; once the enemy is denied, it is not deterred despite the possibility that the next attack may be.[26] Ultimately, Harknett argues that denial does not influence the decision calculus of the enemy by failing to threaten what the attacker covets, nor change their behavior from aggressive to non-aggressive.[27] This is the case even if the attacker's objectives are more difficult to achieve due to the denial strategies in place. Harknett's assertions are echoed by other cyber security scholars who believe that punishment should trump denial in an attempt to establish a formal deterrence strategy. For example, Arquilla argues:

> "the prospect of warding off a bloody fight by the non-lethal means of disrupting military command and control via cyberspace weapons is one that should not be passed over easily."[28]

While Morgan asserted that punitive deterrence is difficult to implement, Harknett argues that objective denial lacks the influential factor necessary to change an attacker's behavior. Separately these strategies are flawed and can be circumvented by those meant to be deterred. However, if combined, the two strategies can mitigate the weaknesses of the other and successfully influence the decision calculus of an attacker. The idea of combining the two strategies emerged in 2003 during the George W. Bush administration when cyber deterrence was addressed as a priority national security concern. In 2003, the Bush administration published the National Strategy to Secure Cyberspace (2003), a

---

[26] Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. "Leaving Deterrence Behind: WarFighting and National Cybersecurity." *Journal of Homeland Security and Emergency Management* 7, no. 1 (2010): 17. doi:10.2202/1547-7355.1636.

[27] Ibid.

[28] Arquilla, John. *Worst Enemy: The Reluctant Transformation of the American Military*, 129. Chicago: Ivan R. Dee, 2008.

document released by the White House acknowledging the difficulties in creating cyber deterrence and recommending a combined approach that focused on objective denial and the use of retaliation in the event of a cyber-attack. These recommendations were also echoed within the National Strategy for Homeland Security (2002/2007) and the U.S. National Security Strategy (2002/2006). Despite the attention given towards establishing a national cyber deterrence strategy, the Bush administration failed to actually create a comprehensive framework. Cyber security scholars conclude that the U.S. must deter its enemies, not dissuade them, by force if necessary. This strategy became the foundation for the Obama administration's approach to cyber deterrence. [29]

The Obama Strategy (2009-Present)

This new consensus achieved by cyber experts has pushed cyber deterrence in the direction of punitive deterrence. This direction has ensured that a degree of deterrence can be established as deterrence through punishment offered the United States the ability to threaten and attack what their enemies hold dear in response to a cyber-attack. With the stage set for the establishment of a formal cyber deterrence strategy, the Obama administration began to work on a comprehensive framework through the Cyberspace Policy Review released by the White House in 2009. In this 2009 review, the White House stresses the need for a forthcoming cyber deterrence policy needed to safeguard critical infrastructure. Harknett's analysis of the Cyberspace Policy Review goes on to say that the U.S. strategic option should be replaced by a war-fighting posture with the

[29] Stevens. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

mission to respond to cyber aggression.[30] Two years later, the Obama administration released the *International Strategy for Cyberspace* reflecting Harknett's ideas (2011).

In the *International Strategy for Cyberspace*, it can be seen that the White House had paid close attention to the history of American cyber deterrence, clearly separating dissuasion from their definition of cyber deterrence. In the section pertaining to dissuasion, the White House proposes two approaches designed to make the United States more robust to attack and dissuade enemies from attacking through cyberspace. One approach focuses on risk mitigation and response through improving network security and reducing vulnerabilities. The second approach focuses on international collaboration and improving detection for vulnerable national assets and infrastructure such as the Bulk Electric System. However, the White House adopted the position of the subject-matter experts in cyber deterrence by relegating robustness and resiliency as a tactic of dissuasion. Instead, the White House recognized the need to send a costly signal to its enemies abroad by targeting what their enemies cherish; their desire to avoid a direct conflict with the United States. As such, the White House proposed a deterrence strategy that echoed an offensive approach. [31]

According to the International Strategy for Cyberspace, the U.S. reserves the right to investigate, apprehend, and prosecute any attacker attempting to intrude upon domestic and international networks. Furthermore, the strategy also states that the United States

[30] Ibid.

[31] Obama, Barack H. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* Executive Office of the President of the United States, 2011. Accessed March 15, 2013. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

shall respond to any hostile acts towards the United States in cyberspace through any and all necessary means. This includes diplomatic, economic, informational, and military or conventional capabilities. However, the document also claims that any response shall be appropriate and consistent with applicable international law. As previously said, this is the closest that the United States has ever reached to creating a comprehensive cyber deterrence strategy, but nonetheless it is not a comprehensive cyber deterrence strategy. As with much of the U.S. government's approaches to dealing with defense related issues, the White House took an evasive approach to outline its strategies for the sake of operational security, thereby leaving doubt of any clear strategy to deter cyber-attackers.[32]

The Realities of U.S. Cyber Deterrence

According to the White House and the Defense Department, the United States will retaliate in kind as applicable within international law in the event of a cyber-attack against it. Despite this strong overt signal for retaliation, the United States continues to be attacked on a daily basis by state and non-state actors. What is remarkable is the fact that there haven't been any overt responses to punish enemies and signal to others the same costs of waging a cyber-attack publically. If the threat of punishment as discussed through the history of U.S. cyber Deterrence is designed to deter cyber-attackers, why haven't their decision calculus changed? Attacks continue to occur against critical infrastructure and networks such as the BES, Wall Street, and the Pentagon's SIPRNet on a daily basis. Countries have now begun to create units within their state militaries

[32] Ibid.

designated to conduct cyber warfare, defense, and espionage. Criminal syndicates and hackvitist groups continue to roam free across the world and cyberspace while targeting America's private sector and causing billions of dollars in damages every year. It is clear that deterrence is not working, but the question remains as to why deterrence has failed. Is the lack of overt retribution the real cause? Is it the lack of a domestic precedent similar to the Stuxnet attack in Iran? Mitigating the failures of U.S. cyber deterrence will require a reexamination of what deterrence truly is and how it can be applied to cyberspace.

Chapter 3: Defining U.S. Cyber Deterrence

In examining the current U.S. cyber-deterrence strategy, this thesis concluded that the current strategy is ineffective for a number of reasons. First, the fact that the United States is attacked in cyberspace on a daily basis by rival state and non-state actors through cyberspace indicates the current strategy is not working (i.e. deterrence is not effective in preventing attacks). Second, for the United States to respond against an attacker indicates that deterrence has not been achieved. Based on these assumptions, where did the current strategy go wrong?

The nature of cyber-attacks against the United States indicates that deterrence is not something that can just be suddenly established between two parties since these attacks are on-going. Instead, deterrence must be achieved both horizontally and vertically against state and non-state actors. Re-establishing a new USCDS will require the United States to persuade its enemies that it is in their benefit to cease all cyber-attacks. The first step is establishing a deterrent that will emphasize the cost of an attack is greater than any benefit. This will change the enemy's behavior from one of aggression to that of being deterred. Once cyber-attackers have ceased, the second step is to ensure that cyber-attackers will not revert back to their aggressive behavior and resume hostilities. Thus, cyber-deterrence, identical to conventional deterrence, requires the United States to modify the enemy's behavior to preserve a balance of power and avoid conflict. If the current strategy does not fit the operational definition of cyber deterrence

then what should an alternative strategy look like? To answer this question, we must first review what deterrence is and how it can be achieved in cyberspace.

Deterrence According to Robert Art

Robert Art, one of the most influential Cold War scholars, saw deterrence as a means to prevent an enemy from behaving in an undesirable fashion. To influence this behavior to reflect the interests of the state, Art argued in his famous article *To What End Military Power* that punishment is the only means to maintain enemy behavior once it has initially been deterred. In essence, deterrence is the threat of retaliation, a central theme within the present Obama Administration's strategy for cyber deterrence. The key behind successfully deterring the enemy is to convince the adversary that the target has the will and means to punish the would-be attacker. Art argues that such a strategy is peaceful in nature, as it does not involve kinetic action but rather the threat of it. Should the threat be carried out, or if the threat fails to deter the enemy, then deterrence has failed. Therefore, the threat is made with the intent that it not be carried out, but the quality of the threat is dependent on the perception of would-be attackers that the threat of punishment is credible. The threat alone is meant to deter action for fear of the consequences. Ironically, the success of deterrence can only be judged successful if there is no attack that requires the use of retaliation or the use of the deterrent.[33]

In addition to deterrence, Art also argues that the decision calculus of the enemy can be influenced by a strong defensive posture, Art argues the defensive use of force is used to mitigate or prevent attacks from occurring by denying the objectives of the

[33] Art, Robert J. "To What Ends Military Power?" *International Security* 4, no. 4 (1980): 3-35.

enemy. This can be used prior to an attack in the form of a pre-emptive or preventative strike, or after an attack has occurred through second strike capabilities. In the latter, a second strike is only possible if the attack can be absorbed and the state is resilient enough to mobilize its forces for a retaliatory attack. In short, this strategy argues that "the best defense is a good offense." Art emphasizes a clear difference between the strategies of defense and deterrence, but his characteristics of the two prove that they can be complimentary. On the one hand, Art argues that defensive strategies are characterized by defensive preparations and their dissuasive value. On the other hand, deterrence is characterized by altering the enemy's behavior through any means necessary. Therefore, a defensive type of force can be operationalized in a manner to change enemy behavior. Following this logic, a defensive strategy involves aggressive militarization and preparation. Increasing the state's resiliency through a defensive posture increases its ability to absorb an attack from the enemy. When this is realized by the enemy, the objectives of the attacker have been denied due to the fact that there is no incentive to waste resources on an attack that will not yield any benefit and possibly lead to the identity of the aggressor. Furthermore, the defensive posture made possible by a robust defensive strategy increases second strike capabilities if there is a need to use them. This second strike capability is a strong deterrent and can greatly influence the decision calculus of the enemy to change its attacking nature when it remains as a useable option by the target state.[34]

[34] Ibid.

Without a defensive strategy, an attacker can easily destabilize a target's second-strike capabilities if it knows where to look. The fact that a defensive posture increases the survivability of a second-strike makes punishment as a component for denial more credible. Meanwhile, the U.S. does not need to be concerned with its punitive capabilities when it can ensure that they will still be operational when retaliation is necessary. Thus, the combination of a defense posture with a punitive element can serve as a strong foundation for an over-arching deterrence framework where a punishment is not interchangeable with denial, but merely a part of it.

Deterrence According to Robert Pape

In the influential book *Bombing to Win,* Robert Pape offers an understanding of achieving deterrence and coercion through the use of strategic air power. Before clarifying what deterrence actually looks like, Pape makes a distinction between coercing an enemy and deterring it altogether. Both concepts focus on influencing the enemy's decision-making calculus, but only coercion forces the opponent to change its behavior. Deterrence, on the other hand, aims to preserve the status quo by discouraging the enemy from altering its behavior in a way that may threaten the balance of power. In the case of U.S. cyber security, deterrence is achieved when the enemy is not launching waves of cyber-attacks against critical American infrastructure. Coercion, nevertheless, is achieved when the enemy is forced to change its behavior and cease its cyber-attacks. Both strategies may seem similar, but threats that deter do not necessarily coerce and vice versa. According to Pape, the reason behind the disparity is due to the defender's greater affinity for their territory than the attacker, and thus the defender will go to greater

lengths to preserve it. Since the attacker is more likely to disturb the status quo and be more risk-averse than the defender, defenders are more willing to preserve their territory than attackers are willing to take it. As a result, defenders are more likely to deter attackers as a result of their greater threshold for suffering.[35]

To preserve the balance that Pape identified as the foundation for deterrence, states can utilize two different approaches. The first approach is through the use of punishment, in which the state seeks to inflict costs greater than the benefits gained by the attacker. This is basically the USCDS of the Obama Administration discussed in Chapter 2, in which the United States increases the costs of attack through the promise of retaliation. The second approach is the use of objective denial as the primary alternative to cyber deterrence through punishment. Pape argues that the most effective manner to deter a conventional enemy is through objective denial as opposed to punishment. Punishment, according to Pape, is only effective in instances where nuclear weapons are a military factor. In non-nuclear environments, denial is viewed as the prime strategy. Denial is achieved when the target or the attacker is undermined to the point where it begins to doubt its own strategy. In cyberspace, however, denial is not interchangeable with deterrence but merely a form of it.[36]

Deterrence According to the U.S. Military

Similar to Art and Pape, the U.S. Department of Defense has defined deterrence as the "prevention from action by fear of the consequences." The definition outlined by

[35] Pape. *Bombing to Win*. 4-6.

[36] Ibid., p. 9-10.

Joint Publication 1-02 in the Department of Defense Dictionary of Military and Associated Terms goes on to say that "deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction." Based on this definition, there are two factors that serve as the foundation for deterrence. The first is the creation of a credible threat, whether in the form of kinetic capabilities or the ability to deny the enemy's objectives. The second is the ability to carry out the credible threat with available resources. Deterrence is only successful when the state is able to convince the attacker that the perceived risks to the attacker are greater than the possible benefits and the consequences are inevitable. This is achieved when a costly signal of retaliation is sent to possible attackers weighing the decision to attack. However, deterrence fails when the credible threat is unable to prevent the attack from occurring. Ultimately, the aim for the United States is to be able to influence the enemy's behavior through a psychological effect created by a clear response protocol.[37]

Deterrence in Cyberspace

With the definition of deterrence clearly identified, the next question to answer is whether deterrence can effectively center the U.S. cyberspace strategy. Additionally, the question must be asked whether deterrence through punishment is more or less effective than objective denial and a strong defensive posture. Chapter 3 will now discuss what an effective USCDS must look like and whether punishment, denial, or a balance of the two is the best strategy to implement for a new U.S. cyber deterrence strategy.

---

[37] Lowther, Adam. *Deterrence Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century*, 165-166. New York, NY: Palgrave Macmillan, 2012.

What is Cyber Deterrence?

However, what of those who do not fear retaliation or who work within borders of a state willing to protect them? Similar to the concept of classical deterrence, Richard Andres argues that cyber-attackers must be convinced that the costs of an attack are far greater than any derived benefits. Like deterrence in the physical world, this is achieved by denying the attacker's objectives and preserving the threat of retaliation. Based on Andres' depiction of deterrence in cyberspace, combining denial and punishment can make deterrence viable in the digital world just as it is in the physical world. However, in order to achieve cyber deterrence, both denial and punishment strategies must overcome eight evaluative criteria affecting cyber deterrence.[38]

The Attribution Problem

Like any crime committed by one actor against another, the target can only respond against the attacker if it can successfully attribute the attack. Attribution in the physical world can be an issue when attacks are unclaimed or committed on a small-scale. Regardless, it is clear that a physical attack taken against a target that a perpetrator would be identified over time. In cyberspace, it is much easier for attackers to conceal their identities and origins.[39] This anonymity makes attribution difficult to achieve given the number of forms an attacker can take. For example, an attacker can be a state actor or an element of a national government with authorization to use cyber-attacks against a

[38] Andres, Richard B. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012. 89-100.

[39] Ibid.

rival state, such as the Chinese hacking group APT1.[40] APT1, also known as Unit 61398 of the People's Liberation Army of China, has been attributed in a series of attacks on U.S. critical infrastructure and media outlets.[41] However, attribution was not achieved until February 2013 despite hundreds of data breaches.

A state does not need to use its military capabilities for it to be implicated in a cyber-attack. A state-sponsored cyber-attacker can be a single perpetrator or a group of freelance hackers supported by a national entity thus a state can maintain deniability. An attacker can also be a rogue element seeking to undermine their government for political or nationalist reasons. Non-state cyber-attackers can also emerge in multiple forms. An attacker can be a criminal enterprise seeking to profit from the destruction of U.S. critical infrastructure. They can also include fundamentalists, terrorists, or hacktivists waging a cyber-attack in the name of an ideology. Finally, an attack can originate from a single hacker contracted by any of the entities discussed above. It is also possible for attackers to disguise their true identities by masquerading as another state or non-state actor. Given the wide range of possible attackers, having the tools to successfully attribute an attack is necessary for the ability to retaliate. [42]

The Contestability Problem

Even if targets can successfully identify their attacker, they must be able to prove to the international community the attack is definitive enough to merit retaliation. An

[40] Ibid.

[41] Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." Accessed May 15, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[42] Libicki, Martin C. "Cyber Deterrence and Cyberwar." RAND Corporation. Last modified 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

accusation is only worth making when there is enough evidence to incriminate the perpetrator without question and fully justify the action. The lack of evidence grants the perpetrator the opportunity to contest the accusation of attack without incurring punishment from the target, as the target risks losing its social capital if it responds while uncertainty regarding the identity of the perpetrator remain. Compiling credible evidence is vital as it signals to the world the perpetrator's acknowledgment in its role in the attack rather than it just being accused by the target. Thus, contestability is another criterion for the establishment of a deterrence strategy. Limitations in attribution can also impact contestability and weaken the effectiveness of the deterrent. Without clearly identifying the attack, a target is unable to weaken the enemy's contestability and lead to further attacks from state and non-state actors who can circumvent a target's forensic capabilities. [43]

The Code of Silence Problem

To successfully persuade a rival to maintain its deterred behavior, this requires overt and costly signals. Without overt signals, potential attackers are completely uncertain if there is a protocol for retaliation, causing an increase in cyber-attacks. Governments and companies compound the issue given the desire to keep offensive and defensive successes a secret in order to preserve their effectiveness. When capabilities are

[43] Goodman, Will. "Cyber Deterrence: Tougher In Theory Than In Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102. Accessed January 15, 2013. http://0-go.galegroup.com.bianca.penlib.du.edu/ps/retrieve.do?sgHitCountType=None&sort=DA-SORT&inPS=true&prodId=AONE&userGroupName=udenver&tabID=T002&searchId=R1&resultListType=RESULT_LIST&contentSegment=&searchType=AdvancedSearchForm¤tPosition=1&contentSet=GALE%7CA243958196&&docId=GALE|A243958196&docType=GALE&role=.

revealed, attackers and defenders alike will discover ways to exploit their opponent's vulnerabilities. Revealing the extent of a cyber-attack can also have disastrous political and economic consequences. Private companies who are overtly attacked will lose the confidence of their clients and shareholders. OBES who have SCADA systems manipulated by a cyber-attacker find themselves scrutinized by lawmakers and are forced to implement costly reforms. Even when the intelligence community or the military becomes the victim of a cyber-attack, such as the penetration of the U.S. Department of Defense's classified SIPRNet, it causes a loss in credibility with stakeholders. With this in mind, both public and private organizations have an incentive to act evasively regarding cyber-attacks for political, economic, and security reasons. This results in the lack of developing new and effective means to combat cyber-attackers in the future. Furthermore, an overt deterrence strategy similar to the one used for nuclear weapons and mutually assured destruction during the Cold War is difficult to achieve due to the inability to send cyber-attackers a costly signal of retribution.[44]

The Regulation Problem

Much of the critical infrastructure in the United States is owned and operated by the private sector. As such, defending these vulnerable industries is difficult to do without developing a public-private partnership. In some cases, Andres argues, government regulation is an option to improve the protection of critical infrastructure made vulnerable by cyber-attacks. Regulations such as improving detection standards or mandating the use

[44] Andres. *Cyberspace and National Security*. 93.

of isolated intranet systems can provide a significant advantage to the defense of infrastructure. However, to do so will result in the imposition of great economic costs that owners of U.S. critical infrastructure consistently lobby against. With the private sector unwilling to pay the costs to effectively protect vital industries, deterrence suddenly lacks credibility given the lax security of critical infrastructure. The degradation or destruction of such infrastructure can cause severe implications for the American population and weaken the second-strike capabilities of the United States by reducing its flexibility for response. Therefore, it is difficult to deter a cyber-attack when it can eliminate second-strike capabilities by targeting specific critical infrastructure, such as the Bulk Electric System.[45]

The Spy-VS-Treaty Problem

When a state is lucky enough to successfully attribute a cyber-attack, it must track the location of its attacker in order to neutralize the threat. Should the attacker be located across state borders, the target must rely on international agreements designed to track and prosecute the attacker for their crimes. This is typically a non-issue when countries cooperate jointly in the tracking and attribution of cyber-attacker. For example, the United States can respond against a non-state actor in an allied state with extradition laws. This becomes an issue when the attacker is located in a country that is unwilling to cooperate or is complicit in the aggression. For example, the Estonian cyber incident in 2007 illustrates the concept of vigilante hackers hiding behind a state actor. In this

[45] Ibid., p. 93-94.

.

instance, Russian hackers attacked Estonian cyberspace in response to a diplomatic incident between Russia and Estonia. When the attacks were traced to IP addresses in the Russian Federation, Estonia's retaliation was stalled in part because of unwillingness by Russia to punish their own citizens or grant Estonian investigators access to Russian cyberspace. If Russia had cooperated with Estonia, it would have left it vulnerable to Estonia investigating the attack and possibly implicating the Russian government in the cyber-attack. Due to Russia's uncooperative nature, Estonia was unable to conduct the forensic analysis it needed to attribute its attack and justify its retaliation. Russia, like many other havens for cyber-attackers, will continue to pose a threat to the viability of punitive deterrence strategies to deter non-state actors.[46]

The Scalability Problem

As discussed in Chapter 1, the void of regulation in cyberspace makes the concept of using social norms to influence behavior unattainable. This also applies to creating norms to address the issues of crime, espionage, terrorism, and warfare in cyberspace. The lack of established norms creates an issue regarding proportionate behavior in response to a cyber-attack. Small attacks with little damage usually do not merit retaliation, but if the United States chooses to respond against insignificant attacks with large-scale capabilities, it runs the risk of waging a disproportionate response.[47] Many states have tried to establish what is considered to be a cybercrime distinguishable from

[46] Ibid. p. 94.

[47] Libicki. *Cyberdeterrence and Cyberwar*.

espionage, terrorism, and warfare. Others, like the United States, reserve the right to use any and all means necessary to address a cyber-attack on a U.S. system. This disparity creates a scalability issue for the United States and other potential targets of cyber-attacks. Does a cyber-attack on Wall Street that causes billions of dollars' worth in damage merit the same punitive response as a rocket attack on American military instillations? The latter example would be considered an act of war whereas the former continues to occur undeterred and without an overt response from the US. In the event that a cyber-attack on Wall Street does merit a response, to what extent can the United States respond?

The main issue regarding the scalability problem is due to its unpredictable effects vis-à-vis conventional weaponry. For example, a tank, nuclear weapon, or even a soldier on the front line can have a predicted effect on the battlefield. On the other hand, a cyber-attack can have widespread intended and unintended consequences. In the case of the Russo-Georgian War of 2008, Russian hackers intentionally defaced Georgian websites and temporarily crippled electronic services in Georgian cyberspace. Russian hackers also implemented time-sensitive viruses that wreaked havoc upon Georgia's cyberspace for weeks after the physical war had subsided. Building a deterrence strategy in cyberspace without clear social norms is difficult. The ambiguous properties of scalability can embolden attackers to use their cyber capabilities with minimal fear of retaliation given the target's fear of inciting retribution and escalating the conflict.[48]

[48] Goodman. "Cyber Deterrence." 102.

Socio-Political and Economic Costs

Warfare is expensive as is the militarization required to prepare for it. The costs associated with attacking enemies, whether in the natural or cyber world, is a considerable factor that can serve as an obstacle to deterrence as well as the costs associated with defense. Reduced public sector budgets can limit the options available to retaliate against a cyber-attack. In regards to building defense for critical infrastructure, much of the financial responsibility is held by private-sector operators. Private companies will not bolster their resiliency without some form of incentive for offsetting the cost. These financial limitations can be exacerbated by strenuous economic conditions that constrain the spending capabilities of public and private sector entities, further increasing the challenge of establishing deterrence with constrained capabilities. Nevertheless, the threat of physical retaliation is likely to be more cost effective than increasing the resiliency of critical infrastructure and networks in the United States. This is because physical or electronic retaliation is less expensive than bolstering defenses for critical infrastructure.[49]

Despite the economic limitations associated with deterrence, socio-political costs that exist. Again, failing to deter an enemy can have consequences against the target population, resulting in grave implications that can threaten financial security, social order, and the lives of civilians. Addressing socio-political costs serves as an additional criterion for the creation of a cyber-deterrence strategy. As such, a national framework for cyber deterrence must also incorporate a contingency plan in the event of its failure.

[49] Libicki. *Cyberdeterrence and Cyberwar*.

Without such plans, socio-political costs can mount and threaten the ability of the target to recover. In addition, cyber-attackers will be emboldened to carry out further strikes as the weakened target is pre-occupied with mitigating the damaged incurred from the initial attack.

An Alternative Strategy to Punishment: Robustness

With a firm understanding of the factors that contribute to the effectiveness of cyber deterrence, an alternative USCDS must be created to avoid the problems associated with deterrence via punishment. Policymakers should reintroduce the concept of objective denial to be used as the center of a new USCDS. In contrast, past scholars have dismissed objective denial as a dissuasion tactic and nothing more which has been echoed by the Obama Administration. However, when objective denial takes the form of the defensive use of force, the ability to absorb attacks increases the likelihood of deterrence. As such, defense-in-depth strategies based on denying the aggressors' goals can be used as an alternative deterrence strategy to address the eight criteria impacting the effectiveness of cyber deterrence. A deterrence framework based on denial also addresses the realities of cyber security. It is based on the assumption that not all attacks can be prevented and defensive capabilities cannot evolve as quickly as offensive capabilities. The question remains, however, what would a U.S. strategy based on objective denial look like for cyber deterrence?[50]

[50] Ibid.

To achieve deterrence in cyberspace requires the acceptance that deterrence does not solely depend on a target's obligation to retaliate.[51] Threatening to punish a cyber-attacker into compliance is ineffective. Rather than threatening to punish would-be attackers, the United States would be better served to prevent attackers from meeting their objectives through an array of capabilities. As discussed previously, denial as used here is not a substitute for deterrence but rather a form of it. One way to achieve deterrence is through the implementation of a strategy centered on establishing robustness. Robustness is a three-pronged denial strategy that consists of defense, redundancy, and the preservation of the option for retaliation.

Defense-in-Depth

In 2006, the Critical Infrastructure Task Force (CIFT) of the Homeland Security Advisory Council (HSAC) argued that critical infrastructure protection measures were: "focused too much on protecting assets from terrorist attacks and not focused enough on improving the resilience of assets against a variety of threats."[52] Denying the enemy's objectives in cyberspace will require the United States to combine mainstream notions of U.S. cyber security with unconventional approaches for cyber resilience. To operationalize this union, the United States must implement a cyber-strategy that includes a strong defense-in-depth component. In the military sense, defense-in-depth is best illustrated through the metaphor of a medieval castle and its defense against invaders.

---

[51] Cooper, Jeffrey R. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 106. Washington, DC: Georgetown University Press, 2012.

[52] Moteff, John D. *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*. Congressional Research Service, 2012. Accessed April 28, 2013. http://www.fas.org/sgp/crs/homesec/R42683.pdf.

A castle consists of multiple layers of defense designed to provide contingencies in the event of the failure of any single defensive layers. The multiple layers ensure that the enemy will have to devote much of its resources to get to reach the castle's inner sanctum and claim whatever prize the castle is defending. To reach the prize, the invaders will be forced to encounter the first line of defense consisting of a barrage of arrows fired by archers on the castle walls. Next, the invaders must cross the moat surrounding the castle since the drawbridge has been raised. Once the invaders reach the outer wall, they must scale it, tunnel under it, or blow a hole in it to cross the barrier. However, crossing the outer wall only leads the invaders to cross the gap to the inner wall laden with traps and defending soldiers. Even if the invaders make it to the inner wall, they are uncertain of the challenges that lie ahead under the harassment of the defenders. There can be additional walls, traps, soldiers, and even the keep at the very center. Demoralized from the challenges that lie ahead, attackers are faced with the decision to press on or retreat to the safety of their encampment. If the attackers retreat, the defenders have successfully denied the objectives of the enemy by trading space for time, protecting the key resources within, and retaining control of the environment.[53]

Not only is defense-in-depth a formidable strategy for warfare, but it can be a powerful component for a denial-based U.S. deterrence strategy. Like the castle metaphor, the United States must increase its resilience of its systems by implementing multiple layers of physical and cyber defenses. Bolstering preventive and detection capabilities increases the difficulty and reduces the effectiveness of a cyber-attack. This

[53] Smith, Randy F. "Defense in Depth." *Windows IT Security* 5, no. 11 (2005): Accessed May 3, 2013. http://0-search.proquest.com.bianca.penlib.du.edu/docview/215123642.

is due to the increased likelihood of a cyber-attacker getting caught in the act, the possibility of preventing the attack from reaching its target, and the increased likelihood of identification or retaliation. Creating multiple defensive barriers mirrors the use of defense-in-depth in a conventional sense by trading cyberspace for time. As time elapses, the target can improve its chances to attribute the attack and force the disclosure of intent by the attacker while also denying the aggressor's goals for the attack. An added benefit of the defense-in-depth strategy is that once disclosure has been achieved, the target can scale its response appropriately with minimal risk for escalation and retaliation from another state. Although the use of a defense-in-depth framework can have the potential to change an attacker's behavior, it alone cannot do so due to the realities of cyber security discussed in Chapter 1. With this in mind, the United States must accept that attacks will circumvent the defensive layers proposed above. As a result, the key to denying the enemy and rendering attacks ineffective is to ensure a layered defense is resilient enough to absorb an attack.[54]

Redundancy

Making a system more robust will also require making the system as a whole as redundant as possible. Redundancy allows the target to absorb any attack upon the system while minimizing its effects. Thus, if defenses are breached, redundancy minimizes the consequences and may even deny the attacker the effects they hope to achieve while preserving the second-strike capabilities. An illustration of the advantages of redundancy can be seen in the engineering of airplanes. The aviation industry implements a redundant

[54] Cooper. *Cyberspace and National Security*. 113-114.

approach for security in order to preserve the integrity of airplanes.[55] Airplanes are designed to reflect a set of small, diverse, and coordinating functions.[56] Each system takes into account the implications of a system failure on other systems.[57] Multiple redundancies are incorporated within the system to mitigate failures and ensure survivability.[58] The extent of redundancy in aviation is detailed in Appendix H of the FAA System Safety Handbook:

> "For safety critical command and control functions: a system design that requires at least three independent failures, or three independent human errors, or a combination of three independent failures and human errors."

A similar approach must be implemented to protect critical infrastructure in the United States. If there are Chinese cyber-attacks on the electric grid or on American financial institutions that go undetected, U.S. systems must be able to absorb the attack and isolate damage. Like in the aviation industry, the U.S. critical infrastructure must be able to withstand system failures and quarantine infected areas while preventing the total collapse of the system. The U.S. will be able to absorb attacks while sending a powerful signal to cyber-attackers that their objectives have been denied.

---

[55] Overman, Thomas M., Terry L. Davis, and Ronald W. Sackman. "High Assurance Smart Grid." Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. Last modified 2010. http://0-delivery.acm.org.bianca.penlib.du.edu/10.1145/1860000/1852734/a61-overman.pdf?ip=130.253.4.14&id=1852734&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1E66739E26778C50D1A135E9E0C10ED60&CFID=234176311&CFTOKEN=63291536&__acm__=1374080167_a9efbb782636cad50c2f401490e3a2b4.

[56] Ibid.

[57] Ibid.

[58] Ibid.

The Option of a Tailored Response

In addition to denying the enemy's objectives, physical and network redundancy in critical infrastructure will preserve the U.S. ability to retaliate and enhance its deterrent with the threat of punishment. Cyber-attacks against the U.S. will be mitigated, ensuring the survival of second-strike measures, whether physical or through cyberspace. This fosters the opportunity for a tailored response, where punishment is merely an option based on the scale of the attack and the survival of second-strike capabilities. Robustness allows the U.S. the time, resources, and capabilities to absorb and analyze an attack in order to identify the perpetrator and plan its response. Rather than immediately responding, as argued in the current strategy, the U.S. can tailor responses to be executed at the most advantageous moment. Specifically tailoring responses based on information collected through defense-in-depth and redundancy measures permits the U.S. to address its cyber deterrence criteria. Finally, the objective denial made possible by layered defenses and redundancy in conjunction with the threat of tailored retaliation allows the United States to effectively deter cyber-attackers contemplating a strike against the United States.

Conclusion

In this proposed strategy of U.S. cyber deterrence for robustness Chapter 3 has identified the benefits of substituting a purely punitive approach to deterrence with an alternative based on robustness; confronting would-be attackers with both meaningful and frustrating defense in depth and objective denying redundancy. Rather than punishing cyber-attackers, the United States can place itself in a position to absorb attacks through a

layered defense. The greater the defensive posture, the lower the probability that a cyber-attack will be effective.[59] Additionally, a layered defense will safeguard the United States' second strike capabilities and permit a tailored response if needed. However, the question remains as to how robustness can be implemented as a cyber-deterrence strategy. What would it look like to a cyber-attacker seeking to strike at critical infrastructure? Chapter 4 will illustrate how robustness can be used to safeguard the Bulk Electric System and deter potential cyber-attackers.

[59] Libicki. *Cyberdeterrence and Cyberwar*.

Chapter 4: Applying Robustness to the Bulk Electric System

As discussed in Chapter 2, thousands of cyber-attacks occur daily against the United States confirming that the current strategy is unsuccessful. Chapter 3 identified factors that determine the effectiveness of cyber deterrence and offered a new USCDS based on denying enemy objectives. Chapter 4 will illustrate how this new cyber strategy based on denial deterrence will be implemented using the Bulk Electric System (BES) as an example to deter cyber-attackers.

A cyber-attack against the electric grid is designed to gather information, destroy infrastructure, disrupt energy services, or a combination of the three. Thus, increasing resiliency requires an electronic and physical approach to security. Once operators of the OBES are robust both in cyberspace and the physical world, these firms can withstand any attempts to undermine the BES. When a cyber-attacker is denied the opportunity to achieve its objectives to disrupt the BES, they will be deterred realizing that they are wasting resources on objectives that cannot be met. As a result, some attackers will seek to exploit or attack another target that is more impuissant than the one denying their objectives and draining their resources. Other attackers will simply quit after realizing that their goals are unattainable. The critical factor in changing the enemy's behavior is to signal resiliency through the adoption of robustness as a USCDS. Doing so will mitigate attacks on the BES and other critical infrastructure while denying cyber-attackers the motivation to strike.

Achieving robustness in the electric grid requires a multi-phased defense-in-depth strategy designed to absorb cyber-attacks and increase the ability for attribution. In regards to the BES, robustness will incorporate both physical and cyber security measures to better protect grid components. Such measures include securing both the physical and digital perimeter of the electric grid, protecting data and services, and increasing redundancy. Maximizing the effects of robust deterrence can only be achieved by implementing all three components of this USCDS for the electric grid. This ensures the ability for the grid to absorb and mitigate cyber-attacks while simultaneously gathering information for attribution purposes and optional retaliation.[60]

Phase I: Layered Defenses

Protecting the electric grid from malicious cyber-attackers begins at the security perimeter of each SCADA system and its connected infrastructure. The first phase of robustness in the BES involves a mixture of detection and prevention measures. As noted in Overman utility defense in depth model, boundary protection measures such as physically securing electrical transmission and setting traps to lure cyber-attackers is the first-line of defense for the BES. Other layers of defense include designing safeguards to protect services and data of the OBES from physical and electronic intrusion from external and internal forces, this includes the idea of an internal threat is critical to ensuring the reliability of the BES.[61]

[60] Ibid.

[61] Overman. "High-Assurance Smart Grid."

Perimeter Security

Among the most vulnerable components of the electric grids are remote terminal units (RTU). RTUs can easily be accessed since there is little security in place to protect them from external tampering. For example, the Smart Grid and its Smart Meters have emerged as a innovate means to increase the efficiency in the electric grids. Meters are connected remotely to SCADA systems to allow home owners to control and monitor their energy usage. Smart Meters are typically located along the outside walls of private homes, and are typically encased within a metal box and secured with a padlock. For cyber-attackers unwilling to infiltrate the Smart Meter remotely, they can easily access the meter by simply removing the lock. Once the attacker has gained access to the meter, it can easily manipulate the system to attack the private home owner or establish a connection with the regional SCADA system to strike from within the system. Likewise, RTUs in remote areas are just as insecure as Smart Meters. Despite the lack of densely populated areas, RTUs are still vulnerable to cyber-attackers willing to seek out and exploit units in rural areas. These units are typically defenseless or are defended by a fence and a padlock. Therefore, this first line of defense is physically vulnerable and needs to be secured from unauthorized physical or remote access.[62]

Studying Cyber-Attacks in Real-Time

Another way to defend the proximity of the electric grid from cyber-attacks is to establish traps known as a Honeypot. This trap is designed to detect, deflect, study, and in certain cases counter cyber-attacks upon information systems. Honeypots can emerge in

[62] U.S. Department of Energy and the North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*.

many different forms, but function with the same purpose. The use of a Honeypot will allow the U.S. to partner OBES to forensically analyze captured malware used by cyber-attackers on the electric grid. OBES typically utilize production Honeypots which gather limited data on malware detected in the company network. These Honeypots are limited in their ability to gather information about attackers to successfully attribute an attack to a single or group of attackers. In contrast, research Honeypots allow for closer monitoring of attackers and attacks and are typically used by research, government, and U.S. military organizations. Research Honeypots come in two forms: high-interaction and low-interaction Honeypots. High-interaction Honeypots create a virtual system identical to the actual system being targeted. The virtual system is used as a decoy to lure attackers into wasting their resources on infecting and destroying the expendable trap as well as possibly exposing their identity. Low-interaction Honeypots replicate the most targeted services within the system and require fewer resources than a high-interaction Honeypot that attempts to simulate the entire system. Nevertheless, OBES would be better served to gather as much information as possible to learn about attacker's signatures and methodology. This is easily achieved through the use of research Honeypots, which hardens the first line of defense against cyber-attackers weighing the risk of being identified through time and resource expenditures. A Honeypot in the electric grid would essentially replicate the system controls of a SCADA or even a specific power node. The cyber-attacker seeking to undermine the system would release their malware on the trap, unaware that they are being monitored; cyber-attackers will continue to expend their resources in the attack and leave a larger forensic footprint. As a result, OBES can collect

more data on the attack and share the information with public sector stakeholders of the BERS, leading to the cooperation of these entities for research, attribution, and response purposes.[63]

Controlling Unauthorized Electronic Access

As previously outlined, Smart Meters are an easy target for malicious attackers to exploit due to their physical and remote vulnerabilities. Although one can easily break apart the metal casing sheltering a Smart Meter on the side of a private residence, it can be just as trivial to access the device remotely given its lack of a firewall. Once inside the Smart Meter, the malicious attackers can use the device as a conduit to target the private residence or direct its attack onto the connected SCADA. This is where electronic perimeter security measures are necessary to deny access to critical systems connected to the Smart Meter. An example of a measure that should be implemented is a host firewall designed to protect device ports and services. Critical systems, such as a SCADA, that are secured by host firewalls will be able to control the flow of data packets originating from remote terminal units. If an RTU, such as a Smart Meter, is compromised, connected systems will be able to block all incoming digital traffic from the corrupted unit. The use of host firewalls and other types of prevention software will add another layer of security for OBES seeking to deny cyber-attackers remote access to their systems from weakly defended units connected to a SCADA or other critical infrastructure.[64]

---

[63] Frederick, Erwin E. *Testing A Low-Interaction Honeypot Against Live Cyberattackers*. 2011 n.d. Accessed March 15, 2013. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA552206&Location=U2&doc=GetTRDoc.pdf.

[64] U.S. Department of Homeland Security. National Cyber Security Division. *Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-In-Depth Strategies*. 2009. Accessed May 1, 2013. http://ics-cert.us-cert.gov/practices/documents/Defense_in_Depth_Oct09.pdf.

Another measure to deny cyber-attackers access to Smart Meters is through integrity measures such as Information-Theoretic Confidentiality (ITC). ITC permits OBES to prevent cyber-attackers from eavesdropping on private customers by remotely accessing their Smart Meter through encoded bits transmitted from the meter. This is achieved by reducing the entropy, the loss of information in a transmitted signal, of Smart Meters so that cyber-attackers are unable to capture information from the transmitted encoded bits. Such integrity measures will increase the difficulty for cyber-attackers to penetrate the BES remotely through RTUs, however it may also drive them to seek out methods to by-pass the electronic security perimeter altogether.

A SCADA can be penetrated accidently or with malicious intent without having to encounter a firewall. One such way is plugging in a USB flash drive that has been accidently or deliberately infected with malware. State and non-state cyber attackers alike can download malware onto USB drives to be transferred onto other systems. For example, the Stuxnet worm attacked Iranian energy infrastructure and was spread from infected computers through USB drives and peer-to-peer sharing. Once a person disconnected an infected USB flash drive from an infected computer, they unknowingly spread the virus to other computers whenever their flash drive was reconnected. OBES can make the same mistake with the BES by bringing their infected flash drives home and connecting them to the company network. As such, access controls must not be limited into the access and monitoring of personnel, but also to the devices that are introduced to a sensitive environment such as a SCADA control room. Thus, a robust OBES will have policies prohibiting any and all flash drives and other devices that can

either physically or electronically connect to a system. Flash drives, personal computers, smart phones and other devices vulnerable to unauthorized access should be completely barred from sensitive areas to ensure maximum internal security.[65]

Host Hardening

While external threats are present from cyber-attackers seeking to penetrate the BES, threats can also exist from within an operator of the BES. OBES must take proper measures to implement internal security measures to protect against disgruntled employees or anyone that can gain access to a company's systems. There have even been instances where dismissed employees still had access to critical systems such as a SCADA despite no longer being employed by the OBES. With this in mind, OBES should implement rigid host hardening procedures as recommended by the Department of Homeland Security (DHS) and/or Department of Defense (DoD). Host hardening procedures are designed to control access to critical systems while reducing their vulnerabilities. One of the access control procedures, for instance, disables unused user accounts while hardening security settings for required services. This ensures that unused services, such as tools, libraries, and files for example, are removed and limits access by certain hosts or IP blocks that should no longer have access a system. Disgruntled employees who have been forced to leave the company will no longer have access to critical SCADA functions from within or without the system. Additionally, OBES should install host-based intruder detection systems, thereby adding additional defensive layers

[65] U.S. Department of Homeland Security. *Malware Infections In The Control Environment*. ICS-CERT Monitor, 2012. Accessed April 2, 2013. http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf.

for detecting unauthorized access to the system. Implementing such procedures will allow OBES to preserve the integrity of data and services while mitigating or preventing insidious attacks. Furthermore, updating systems and removing obsolete services will serve to improve an operator's system performance in addition to security.[66]

Other Access Control Measures

It is imperative for n to create multiple layers of defense to increase the likelihood of detection and the difficulty of BES penetration. OBES would also benefit by safeguarding their data and services from external threats by implementing file integrity checking, host-based intrusion detection systems (HIDS), and secure network management protocols such as SNMPv3 to add additional layers for detection. OBES should also consider encrypting their in-transit and rest data, and router authentication protocols to curb cyber-attackers once they have penetrated a SCADA or other systems.[67] With a consistent threat of attack, OBES must plan for the possibility that a cyber-attacker can navigate past the layered defenses discussed above. Should an OBES fail to detect and prevent an attack from occurring, it must ensure that its system is robust enough to absorb the attack and limit damage locally. Mitigating the implications of a cyber-attack will require the BES to be redundant enough to ensure continuity in the event of attack.

---

[66] Burns, Bryan, Dave Killion, Nicolas Beauchesne, Eric Moret, Julien Sobrier, Michael Lynn, Eric Markham, et al. *Security Power Tools*, 421-430. Sebastopol, CA: O'Reilly, 2007.

[67] Overman. "High-Assurance Smart Grid."

Phase II: Redundancy

Once cyber-attackers maneuver past an OBES's layered defenses and begin exploiting critical systems, the next step is to attack critical systems to cause immediate or long-term BES damage. The cyber-attacker's aim is to access critical system that transfer electrical currents and shut it down in an attempt to cause a power surge. When a power node is destroyed, current power funneled through lines must be re-directed or risk creating a surge with the potential to destroy additional nodes and transmission lines. It is this secondary nature of this attack, after an initial power node or even the entire SCADA system is attacked, which can further damage infrastructure and cause cascading blackouts. In a BES with little redundancy, SCADA's and their supporting infrastructure operate in a linear fashion. Command protocols from the generator dictate the energy flow from substations to field devices through transmission lines. As illustrated by FIGURE 1, energy passes easily from one substation to its corresponding field devices, but not horizontally from field device to field device or substation to substation.[68]

[68] Ibid.

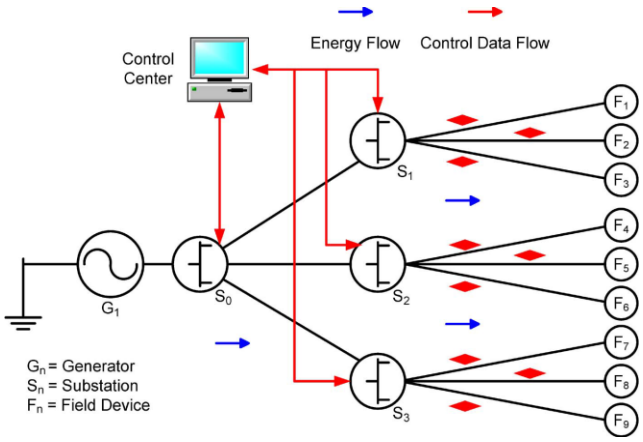

Figure 1[69]

To prevent this from occurring, an increase of redundancy through the building of ancillary power lines is required. When redundancy is established, energy will be able to pass horizontally in addition to its linear path. Redistributing the excess load caused by a downed power line or node through ancillary lines will divert current to other nodes in proximity. This ensures that the energy surge created by a downed transmission line or a cyber-attack can be dispersed across the grid to other substations and field devices, as illustrated by FIGURE 2. In the event of S1's failure, energy can flow directly to S2 as indicated by the blue lines representing the redundancy created by ancillary lines. Energy can then be redistributed across to S3, depending on the capacity of S2, and all of their corresponding field devices to ensure that power disruptions can be mitigated. Under this example, the power outage caused by the failure of S1 will only result in the failures of

[69] Source: figure adopted from Overman, Thomas M., Terry L. Davis, and Ronald W. Sackman. "High Assurance Smart Grid." Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. Last modified 2010. http://0-delivery.acm.org.bianca.penlib.du.edu/10.1145/1860000/1852734/a61-overman.pdf?ip=130.253.4.14&id=1852734&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1E66739E26778C50D1A135E9E0C10ED60&CFID=234176311&CFTOKEN=63291536&__acm__=1374080167_a9efbb782636cad50c2f401490e3a2b4.

F1 and F2, while F3 remains operational through the redistribution of power to S2 and the ancillary line that connects F3 to the substation.[70]

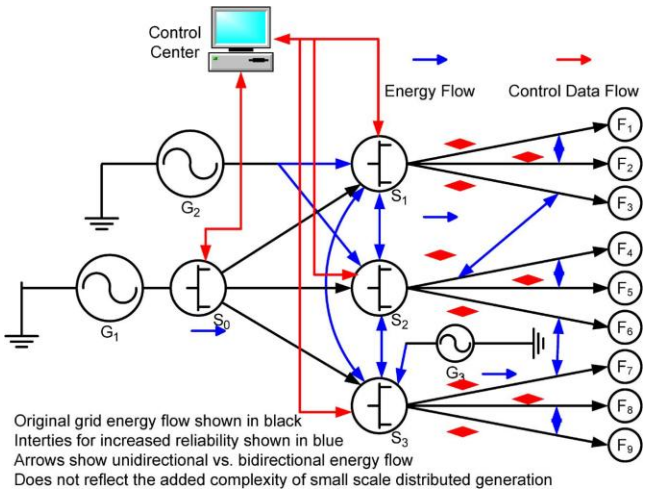

Figure 2[71]

Power nodes rarely operate at full capacity and by spreading out the overload of current across the entire grid with interconnecting lines will reduce the probability for a large-scale failure of the area's power system. Blackouts will be limited to the most severely struck areas, and outages will be relegated to small isolated areas. For example, a downed power line or node can have the potential to cause a city-wide blackout in certain areas of the country. Through the robustness strategy, the excess current will be redistributed through physical redundancy measures to isolate the blackout to a limited area. In this instance, a power outage of city-wide proportions can potentially be limited

[70] Overman. "High Assurance Smart Grid."

[71] Source: figure adapted from Overman, Thomas M., Terry L. Davis, and Ronald W. Sackman. "High Assurance Smart Grid." Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. Last modified 2010. http://0-delivery.acm.org.bianca.penlib.du.edu/10.1145/1860000/1852734/a61-overman.pdf?ip=130.253.4.14&id=1852734&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1E66739E26778C50D1A135E9E0C10ED60&CFID=234176311&CFTOKEN=63291536&__acm__=1374080167_a9efbb782636cad50c2f401490e3a2b4.

to a two-block radius. Ultimately, any large-scale cyber-attacks to disrupt energy services whether at a local or regional level will be mitigated if proper physical redundancies, such as ancillary lines, are in place.[72]

Another method to promote redundancy in the BES is to reduce the interoperability of the grid. Presently, the BES is interconnected so that all segments of the electric grid are linked together in both the physical and digital world. This reality poses a significant risk in the event of a catastrophic cyber-attack with the potential to cause a devastating blackout. As discussed above, a single grid failure has the potential to cause a cascading blackout which can spread across the interconnected grid with devastating consequences. In 2003, for example, grid failures in Ohio led to a cascading blackout that affected the eastern coast of the United States. Citizens from New Jersey to the Canadian province of Ontario were plunged into darkness as the surge in power spread to connected regional grids and forced power plants to go offline. As opposed to building towards an interconnected grid, the United States would be better served to begin diversifying the BES to prevent future cascading blackouts. Creating independent and distinct micro grids will increase the redundancy of the BES as a whole. Each independent grid can have its own unique layered defense system to detect, prevent, and absorb attacks. Such layered defenses can be tailored to the strengths and weaknesses of the OBES's systems. Should one of the micro grids be comprised from a cyber-attack, the BES as a whole can survive unhindered by cascading blackouts or other severe implications. This form of diversity will prevent cyber-attackers from creating

[72] Overman. "High Assurance Smart Grid."

interoperable malware that can affect multiple components of the BES using identical software, programs, and systems. Additionally, isolating the effects of a cyber-attack to a specific area will allow OBES to repair the damage in a timely fashion without factoring the connectivity to other sectors of the BES. Implementing this form of redundancy provides a cost-effective way for OBES to maintain the integrity of their infrastructure while limiting the extent of a cyber-attack. OBES can use available technology, such as synchrophasors, to monitor their segments of the grid in isolation. Synchrophasor technology grants OBES the capability to monitor in real-time to detect disturbances, predict instability, and control the problem. Any intrusion by a cyber-attacker on grid infrastructure using synchrophasor technology will cause irregularities noticeable to monitors. The technology will grant OBES the ability to better identify and defend against cyber-attacks on their isolated systems. Although synchrophasor technology can also be targeted and corrupted by cyber-attackers, OBES can mitigate these vulnerabilities by randomizing and concentrating synchrophasor data packets used for monitoring activities, which will also make the system more redundant. Concentrating multiple data packets into a single line of code and inserting dummy packets to masquerade as relevant data will keep cyber-attackers guessing and force them to devote more resources to successfully corrupt synchrophasor data packets. Creating diversity and redundancy through isolated segments of the BES will ensure that no one cyber-attack can spread across the BES to cause widespread damage at a regional or national level.

In addition to building ancillary lines or a distributed grid, OBES can strengthen their redundancy by working closely with each other and their public sector partners to share intelligence. This concept is not new in a sense that it is presently being advocated by the Obama Administration through the *2013 Executive Order for Improving Critical Infrastructure Cyberspace*. The executive order calls upon a critical infrastructure operator (CIO) to coordinate with the public sector to share classified information pertaining to the protection of infrastructure. In the case of the BES, OBES can benefit greatly by sharing information on cyber-attackers and their capabilities with fellow OBES in addition to the public sector.[73] The notion of information sharing promoted by a presidential executive order fosters a sense of network centric warfare first proposed by Arthur Cebrowski during the late 1990s. Cebrowski argued that giving planes, ships and soldiers to communicate with each other on the battle field rather than transmitting messages to a central command can greatly increase force effectiveness in combating an enemy.[74] This idea creates a shared awareness between forces regardless of their location in order to synchronize their response to a threat. In the case of building redundancy in the BES, synchronizing efforts to address cyber threats builds redundancy as each OBES will increase its defense posture to prevent or absorb an attack. Once a cyber-attack has been detected whether through synchropashor technology, redundant metering, or other forms of redundancy, the targeted OBES can quickly share information gathered with

[73] Obama, Barack H. *Executive Order: Improving Critical Infrastructure Cybersecurity*. Executive Office of the President of the United States, Office of the Press Secretary, 2013. Accessed March 14, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[74] Singer, Peter W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*, 184-186. New York: Penguin Press, 2009.

their counter-parts. Other OBES can use the collected intelligence to adjust their defenses in anticipation of the attack spreading to their systems. With this in mind, OBES across the United States will be on alert and better prepared to defend against future cyber-attacks, which contributes to the redundancy of the BES should the cyber-attack spread from the initial targeted company system.

Phase III: Tailored Response

Once an attack has been launched upon the BES, the United States will find itself with the option to respond if necessary. Layered defenses and the redundancy of the electric grid will allow OBES to either prevent or withstand an attack with little damage to the BES and fewer implications on the public. However, if denying the enemy's objectives does not suffice to deter, the U.S. can retaliate in order to further compel attackers from further aggression. Information collected from defensive layers such as Honeypots, host hardening programs, and access monitoring among other methods will force aggressors to leave behind a larger forensic footprint and allow the United States, as stipulated by the Presidential Policy Directive on Critical Infrastructure Security and Resilience, to resolve the attribution problem. In addition to sharing intelligence, redundancy also allows the U.S. and OBES to observe cyber-attacks in real-time. Observations of behavior and methods during cyber-attacks can permit the U.S. to create an attack profile. For example, private hackers tend to rely on capabilities that are common with hacker communities such as DDoS attacks. In addition, some private hackers tend to focus more on style and seek publicity from their target audiences. In contrast, state-sponsored hackers such as PLA Unit 61398 are less likely to focus on style

and tend to lean towards a methodological or uniformed approach to cyber warfare. As such, state hackers are more likely to be patient in their attacks, waiting for the most opportunistic moment to strike whereas private hackers have a natural curiosity and prefer to explore their targeted system. State hackers also tend to avoid using conventional means such as DDoS attacks and prefer to use more sophisticated methods. This is a typical characteristic of a state-sponsored cyber-attack since private hackers are traditionally unable to finance such extravagant methods. As opposed to striking immediately after an attack, the U.S. will be in a position to tailor a response to its attributed attacker. Robustness, as discussed above, permits the BES to absorb a cyber-attack, allows the U.S. to quarantine infected systems, localize damage, forensically analyze the strike, and ensure that retaliatory capabilities will remain operational. The information gathered in the analysis will not only make attribution easier to accomplish, but also permits the United States to specifically design a response while keeping in mind the strengths and weaknesses of its aggressor. Tailored responses, as discussed in Chapter 3, circumvents the traditional problem areas for cyber-deterrence and allow the United States to punish its attacker with minimal fear of retaliation or escalation. Unlike an immediate response, a tailored response can occur at any point following the attack on the BES that is the most opportunistic for deterrence. Tailored responses would be executed by leading federal agencies with jurisdiction over the domain of the retaliatory strike, such as the NSA or USCYBERCOM in the event of a cyber response. Ultimately, the lack of the preceding phases for robustness would make mitigating damage to the

BES and gathering the necessary information to retaliate difficult to achieve by any number of means.[75]

Conclusion

Utilizing a defense in depth component as part of robustness will deny the objectives of cyber-attackers and create deterrence for future aggressors. Attackers will ultimately waste a substantial amount of their resources in an attempt to achieve their goals in attacking the electric grid. However, this concentrated effort will only result in their attack being absorbed and safely redistributed across the entire electric grid through ancillary lines. Robustness also contains a preventive aspect of its defense in depth component as it directly influences the decision calculus of the enemy, depending on the attacker's aim. Like the first and second phases, the third phase of robustness gives stakeholders the opportunity to counter by tracing the aggressor's signature. Attackers will have to devote more time to by-pass the first and second wave of robustness to even begin attacking the redundant electric grid. As this occurs, it will allow law enforcement agencies and their counter-parts in the U.S. Department of Defense to conduct cyber forensics during and after the attack. As attackers devote more time and resources to the attack, the United States government will have a greater probability to correctly attribute the attack to the correct perpetrator and take appropriate response measures. Cyber-attacks can never be completely prevented; however, the electric grid must be strong enough to withstand those attacks that by pass the first and second layers of robustness

[75] Libicki. *Cyberdeterrence and Cyberwar*.

Chapter 5: Assessing the Current and Proposed Strategies

Robustness can emerge as a formidable USCDS to bolster the electric grid and influence the decision-calculus of cyber-attackers. The proposed strategy outlined in Chapter 4 can be more effective than the Obama Administration's current focus on punitive deterrence? To assess whether the proposed strategy can be more potent in deterring cyber-attackers, this thesis will analyze robustness versus punitive deterrence against the factors influencing the effectiveness of cyber-deterrence. Both strategies will be assessed and a strategy will be less effective if it is consistently plagued by the factors associated with the realities of cyber deterrence. The strategy affected by the least number of factors will be considered the most effective USCDS for the U.S. government and the U.S. Department of Defense to adopt.

Can Attribution be Achieved?

As previously mentioned in Chapter 2, the current Obama Administration's cyber strategy is focused primarily of punitive deterrence. Therefore, the United States will be required to successfully identify aggressors before a response can be made. Even if the government were to concentrate its intelligence resources to properly identifying the attackers, it would not improve its margin of success for attribution. As stated in Chapter 1, the inability to remain on par with the evolution of malware is a glaring vulnerability for cyber-security. This holds true for attribution as well. The future may not make the task of attributing a cyber-attack to a single actor any easier. The most effective means of

attributing an attack to a single actor is to catch the perpetrator in the act. Increasing detection capabilities to ensure a state or non-state attacker is caught in the act can deter attackers from striking for a fear of getting caught. On the other hand, it can also embolden cyber-attackers to cloak themselves further to ensure that they cannot be identified during an attack. If perpetrators are already successfully masking their cyber-attacks, they can just as easily increase their deceptive measures in parallel with increased detection measures by the target country. Once an attack had ended and the diagnostic forensics process has begun, the U.S. government and its private sector partners will find themselves once again in the complex process of determining who was behind the attack on the electric grid.[76]

Unlike punitive deterrence, robustness is not hindered by the necessity of identifying the perpetrator behind a cyber-attack. The defense-in-depth strategy is designed to withstand attacks from both state and non-state actors regardless of the attack's origins. As an added benefit, the strategy can allow the United States to more easily identify its attacker as a means for a tailored response. As more resources are operationalized to damage the BES, the added effort to destroy the grid increases the risk of exposure and attribution for the attacker. With this in mind, the option of attributing cyber-attacks relieves the United States from having to retaliate if it is not in the optimal position to do so. In regards to the attribution problem, robustness provides a clearly defined alternative in addition to the purely punitive deterrence policy.[77]

---

[76] Ibid.

[77] Goodman. "Cyber Deterrence." 102.

Can Cyber-Attackers Contest the Incident?

The current strategy based on punitive deterrence is hindered by the requirement to furnish undisputable proof implicating the attacker in order to justify retaliation. To make matters more complex, cyber-attackers are fully aware of this challenge and will use it to protect themselves from any response by the United States. Cyber-attackers contest or deny their responsibility for an attack, thereby increasing the difficulty to respond since doubt remains regarding the true identity of the perpetrator. Even the risk of covert retaliation for a contested attack can have severe consequences to the United States. This is because without undisputable proof attributing a cyber-attacker, the United States risks losing credibility in the international community and drawing in a third party to the cyber conflict when retaliating. Therefore, punitive deterrence is weak in the sense that it is dependent on not only clearly identifying the exact perpetrator, but to also have the burden to prove it. As such, post-attack efforts made to gather information to remove the attacker's contestability can be time consuming and detrimental to the defense of the Bulk Electric System, given the dynamic environment of cyberspace. As a result, contestability is no longer an issue when response is optional. Robustness provides the ability for the United States to absorb the attack without retaliation. Although proof would be required to justify a tailored response, retaliation is secondary to the United States' resiliency through a defense-in-depth strategy. When the U.S. is in a prime position to retaliate, it can use the data already collected during the absorbed attack to

appropriately tailor a response. As a result, contestability is less of a hindrance for the proposed USCDS rather than the current Obama Administration's strategy.[78]

Must a Response be Scalable?

The next assessment factor focuses on whether the strategies under review are influenced by scalability. The Obama Administration's current punitive deterrent strategy is bound by scalability should retaliation ever be required following a cyber-attack. The United States must determine how to respond to enemy actions given the primary and secondary effects of an attack. The United States has already identified any cyber-attack on the electric grid or any other critical infrastructure as an act of aggression, but will it merit an official declaration of war? In addition, the United States must wrestle with the decision to respond electronically through cyberspace or conventionally through physical firepower. Both approaches will require an appropriate response, a difficult task given the lack of social norms or international regimes to regulate cyber conflicts. Any overwhelming response against a cyber-attacker can be interpreted as excessive by the international community. The United States is forced to remain cautious in the event of retaliation given the potential for scrutiny or the escalation of conflict by state and non-state actors and any other unforeseen consequences. The question of how much force is appropriate for response has yet to be answered by any federal official and casts a cloud of uncertainty on whether or not the U.S. government can immediately respond to a cyber-attack.[79]

[78] Ibid.

[79] Ibid.

Unlike the current USCDS, robustness is not affected by the scalability issue. Unlike punitive deterrence, the new USCDS based on robustness strategy is primarily focused on denying the enemy by absorbing its attack. As such, the strategy is not plagued by the need to respond appropriately to every possible attack against the United States. However, if a tailored response is a favorable option for the United States to undertake, it can be done appropriately as discussed in Chapter 3. In combination with punitive deterrence options, the United States will be under a better strategic position to scale its response by using robustness over punitive deterrence. This will enable the U.S. to collect more information on the attacker during and after an attack. The information can then be used to carefully fashion a response towards the perpetrator of the attack. More importantly, retaliation under robustness is merely an option rather than a key pillar of the deterrence strategy, which does not ultimately undermine by the scalability issue as does the Obama Administration's current strategy.

Will the Code of Silence be an Issue?

The inability to send a costly signal to cyber-attackers severely undermines the effectiveness of punitive deterrence. The willingness by the United States and its private corporations that own critical infrastructure to withhold or conceal instances of attacks emboldens enemies to strike. Although the revelation of a cyber-capability can diminish its effectiveness, so too can the covert nature of cyber retaliation. State and non-state actors as a group are presently unable to realize the destructive potential of electronic or kinetic response by the United States. Compounding the issue is that the United States is attacked electronically on a daily basis. This is similar to the use of atomic weapons on

Japanese cities during World War II. Following the war, the international community became well aware of the destructive potential of nuclear weapons as a deterrent. Deterrence can never be achieved unless the United States can demonstrate its capabilities as it did in World War II and send a costly signal to its rivals that it has the capabilities to punish perpetrators.[80]

The Code of Silence is less of a factor when the United States implements a deterrence policy based on defense-in-depth. Through robustness, the U.S. and private critical infrastructure operators can absorb each cyber-attack without having to divulge the incident in detail. Deterrence is achieved through objective denial rather than punishment. As such, a costly signal is transmitted to the international community through the aggressive hardening of vulnerable infrastructure. Cyber-attackers will factor the resiliency of critical infrastructure, such as the BES, into their decision calculus. Those deterred will view wasting resources as too costly to merit an attack. Attackers who choose to strike will be unsuccessful due to the fact that an attack can be discreetly absorbed and mitigated by the United States. In each case, the desire to conceal a cyber-attack will not undermine the success of robustness in denying the enemy's objectives.

Is the Lack of Regulation an Obstacle?

The current cyber deterrence framework does not rely upon government regulation to secure critical infrastructure. In the absence of regulation, punitive deterrence can remain effective as it is designed to change enemy behavior through costly signals of force. The resiliency of critical infrastructure does not factor into the ability to

[80] Andres. *Cyberspace and National Security*. 93.

threaten cyber-attackers with a kinetic or electronic retribution. As such, the anti-regulation problem is not a hindrance factor for the current cyber deterrence strategy. This issue, on the other hand, can have severe limitations for robustness. The regulation issue can significantly damage the feasibility of robust deterrence and its focus on defense-in-depth and redundancy. Despite the reliability standards created by the North American Electric Reliability Corporation, there is an absence in regulating cyber security for other sectors containing critical infrastructure. Building ancillary lines and or a layered defense as discussed in Chapter 4 is extremely costly, and so are redundancy measures in other sectors. Mandating the development of redundancy and other layered defenses through new U.S. cyber security regulations will increase costs for private CIOs. The private sector is unwilling to cover such costs, especially if there is little opportunity to increase revenue to cover the measures. This explains the opposition of many corporations to regulate cyber security measures in the private sector. So long as regulations on cyber security continue to be opposed by the private sector, the lack of a mandate to build redundancy and resiliency can severely impact the success of robustness as a formal USCDS.[81]

Is the Spy Vs. Treaty Problem an Issue?

Even if the United States can solve the attribution, contestability, and scalability issues hindering its ability to respond against a non-state actor, it must also address the possibility that the cyber-attacker is located in a country unwilling to allow a response against its own citizens. As discussed in Chapter 3, countries are fearful of the United

[81] Ibid., p. 93-94.

States, regardless if the attack occurred under their direction or not. This suspicion of espionage impedes the success of retaliation against non-state attackers hiding within these countries. An example of this is illustrated by the 2007 attack on Estonia's cyberspace by Russian hackers. Despite the fact that the two countries had a formal treaty concerning cross-border crime, Russia objected to any investigation by Estonia or its allies within Russian cyberspace. If Estonia had decided to ignore Russia's uncooperative response, it could have faced escalating the conflict with its larger neighbor. In observing this case, the current cyber deterrence strategy is severely challenged by the Spy vs. Treaty problem as it directly impacts the United States' ability to retaliate against a cyber-attack if it originates from a hostile or uncooperative state. While the punitive deterrence is influenced by this issue, robustness remains unaffected by the cooperative nature of a country hosting non-state cyber-attackers. The strategy's focus on layered defense and redundancy as opposed to an obligatory retaliation renders the problem a non-issue. Using the BES as an illustration, building ancillary lines in the national grid to deny the objectives of cyber-attacker does not require the blessing of a foreign state. Therefore, robustness is the preferred strategy to ensure the resiliency of critical infrastructure regardless of the attacker's origins.[82]

Are there Socio-Political Costs?

When a cyber-attack is waged on America's critical infrastructure, the implications can be catastrophic. Damage can range from blackouts and economic losses and the breakdown of social order. With this in mind, the current strategy can face the

[82] Ibid., p. 94.

entire spectrum of implications in the event that deterrence continues to fail. Regardless if the United States can respond through cyberspace or its military might or economic sanctions, punitive deterrence does not factor in the domestic implications that can possibly occur. Immediate retaliation, as outlined by the current strategy, is externally focused to address the threat against U.S. critical infrastructure and cyberspace. On the other hand, the current strategy is not designed to mitigate any cyber-attack on critical infrastructure or any other targets from within the United States. Logic bombs will not mitigate a breakdown in the BES or the shutdown of the Stock Exchange, but merely serve to incapacitate or destroy the perpetrators of cyber-attacks against the aforementioned targets. As such, the current strategy is negatively impacted by the socio-political costs than can arise when punitive deterrence fails.

The obstacles posed by socio-political costs are less of an issue when robustness is operationalized. Redundancy will allow critical infrastructure to mitigate attacks, limit damage, and reduce socio-political costs. The addition of ancillary lines or a transition to a distributed grid can limit the implications of a cyber-attack on the BES. For example, a blackout can be limited to an isolated neighborhood. As a result, critical services dependent upon electricity will largely remain operational and citizens affected by the cyber-attack will remain relatively unscathed. Based on the defensive components of redundancy, the new strategy for U.S. cyber deterrence is better suited to overcome socio-political costs in the event of a failure of deterrence.

Are there Economic Costs?

As mentioned above, the private sector will be required to offset its costs in order to make critical infrastructure redundant and resilient. The economic costs of such an endeavor are staggering relative to relying on punitive deterrence and the economic costs of retaliation. Using the BES case, expanding the grid in order to create redundancy, alongside all of the costly measures of establishing a layered defense exceed the already budgeted costs of kinetic and electronic retaliation. Furthermore, the economic costs of robustness fall within the responsibility of the private CIOs in contrast to the current cyber deterrence strategy. Therefore, economic costs will emerge as an obstacle that can impact the effectiveness of the proposed USCDS, but are less of a hindrance for the current strategy.[83]

Conclusion

As illustrated by Table 1, the Obama Administration's current strategy is mired by attribution, contestability, scalability, Spy VS Treaty, Anti-Regulation, and the Socio-Political Cost problem. These factors severely limit the ability for the United States to deter its enemies in cyberspace. This assertion is corroborated by the thousands of cyber-attacks that occur on a daily basis against critical infrastructure and networks across the United States.

[83] Libicki. *Cyberdeterrence and Cyberwar*.

Table 1

Addresses Cyber Deterrence Criteria

		Current Strategy		Proposed Strategy	
	Problem	**YES**	**NO**	**YES**	**NO**
OBSTACLES	Attribution	X			X
	Anti-Regulation		X	X	
	Code of Silence	X			X
	Contestability	X			X
	Economic Costs		X	X	
	Scalability	X			X
	Socio-Political Costs	X			X
	Spy vs Treaty	X			X

With the limitations of the current strategy, the United States should turn to a new cyber deterrence strategy that can address the criteria for deterrence outlined in Chapter 3. In Table 1, the proposed strategy can offer the United States the ability to eliminate many of the issues hindering punitive deterrence. Despite the economic cost problem and the necessity for all-encompassing national regulation delaying the implementation of robustness as a strategy, it remains unaffected by the other criteria serving as obstacles for deterrence. As such, this thesis contends that the best strategy to deter cyber-attackers is robustness; where objective denial is combined with a defense-in-depth approach. Furthermore, the implementation of the proposed strategy does not eliminate the need for

retaliation. Although retaliation as outlined in the proposed strategy will be subjected to the same criteria as the current punitive approach, it will less difficult to do so given the greater probability of attributing an attacker made possible by the resiliency and layered defense of targeted critical infrastructure.

Chapter 6: Conclusion and Recommendations

In Chapter 2, this thesis explored the history of U.S. cyber deterrence and concluded that the current strategy is ineffective due to the volume of cyber-attacks against the United States and the undeterred nature of cyber-attackers. Due to the failures of the Obama Administration's USCDS, this thesis proposed an alternative cyber deterrence strategy based on robustness. The proposed USCDS called upon CIOs and the U.S. government to undertake a defense-in-depth approach to deterrence by building layered defenses and redundancy as means to deny the objectives of cyber-attackers. Furthermore, this thesis also argued that increasing the defensive posture of U.S. critical infrastructure would also bolster the U.S. capability to respond against cyber-attackers. Absorbing cyber-attacks will permit the U.S. to mitigate the effects of the attack while collecting information to circumvent the attribution problem and tailor a response to the attack.

In Chapter 4, the BES was used to illustrate the implementation of the new USCDS based on robustness. This thesis described a defense-in-depth approach based on multiple layers of defense, such as Honeypots and Host Hardening measures, to increase the difficulty of penetrating the BES. Furthermore, this thesis proposed a number of redundancy measures, such as the building of ancillary lines, to absorb the effects of a cyber-attack should the preceding layers of defense fail to prevent or detect the attack. The necessity of such defensive layers is due to the realities of cybersecurity; the facts

that a state cannot prevent all cyber-attacks from occurring and that our defensive capabilities will never achieve parity with the consistently-evolving offensive capabilities of cyber-attackers. Implementing robustness in the BES will deny cyber-attackers with limited resources to effectively disrupt and damage the electric grid. Furthermore, the robustness of the BES will grant the U.S. the time and information to tailor a response in the event the new USCDS is unable to originally deny the cyber-attacker from attacking the BES.

Chapter 5 argued that a USCDS based on robustness is designed to overcome many of the obstacles plaguing the Obama Administration's cyber strategy. This is due to the limitations of punitive deterrence in deterring cyber-attackers from striking U.S. critical infrastructure. While serving as United States Deputy Secretary of Defense, William J. Lynn III claimed in an article for *Foreign Policy* on the Pentagon's cyber strategy, "deterrence will necessarily be based more on denying any benefits to attackers than imposing costs through retaliation."[84] Deputy Secretary Lynn also asserts in *Foreign Policy*, "The challenge is to make the defenses effective enough to deny an adversary the benefit of an attack despite the strength of offensive tools in cyberspace."[85] Unlike the Obama Administration's strategy, a new USCDS based on robustness does address this challenge by circumventing the attribution, contestability, and scalability problems that undermines a deterrence-based approach to cyber-attackers. In addition, a robustness-based strategy will also deter cyber-attackers sheltered by rival states and mitigate the

[84] Lynn, William, III. "Defending A New Domain." *Foreign Affairs* 89, no. 5 (2010): 99-100. http://www.usna.edu/AcResearch/NASEC2012/William_Lynn_III_Defending_a_New_Domain.pdf.

[85] Ibid.

socio-political costs of a cyber-attack in the United States. Finally, the new USCDS will create resiliency in U.S. critical infrastructure that will allow public and private stakeholders to discreetly absorb and mitigate cyber-attacks. However, robustness is still limited by the lack of regulation to promote cyber defense in American critical infrastructure and the economic costs to build resilience. As a result, this chapter will discuss available options to mitigate the shortcomings of robustness.

Solving the cost and regulatory problem will require policymakers to issue a mandate or legislation for increased physical and cyber security standards to protect critical infrastructure. A mandate has already been set in the *Executive Order for Improving Critical Infrastructure Cybersecurity* issued by the Obama administration in February 2013. The executive order calls upon CIOs to work with the public sector to develop and implement risk-based standards. Such standards will include methodologies, procedures, and processes to mitigate cyber risks. Regulation over cyber security standards already exists in the BES, with the NERC enforcing industry security standards. With regulation already present in the BES, policymakers must expand to address critical infrastructure owned by private firms in the United States. Implementing regulation on all CIOs will promote a defensive posture for critical infrastructure that will bolster robustness as a cyber deterrence framework and protect vulnerable infrastructure from attack. For instance, regulation can mandate that each CIO must implement a certain level of defense-in-depth for their infrastructure and a certain degree of redundancy must be achieved in order preserve the continuity of service. In the case of the BES, a comprehensive standard can mandate OBES to build ancillary lines to ensure

that no more than 5% of households within a city limit will suffer through a blackout. In addition to bolstering defenses for critical infrastructure, regulation can also provide an avenue to solve the economic cost issue of creating a defensive posture to promote the robustness strategy of cyber deterrence. [86]

However, OBES can only be as effective in securing their infrastructure as the amount of revenue they can collect. OBES cannot devote their revenue to bolstering cyber defenses if they cannot raise their prices to offset the costs of building layered defenses and redundancy. Allowing operators of the BES to raise their prices will ensure that there is a steady stream of income devoted to a strong defense posture to prevent, absorb, or counter an attack against the BES. Federal Energy Regulatory Commission (FERC) and state regulators for the BES understand the need to improve upon current BES infrastructure given the growing threat of cyber-attacks. However, regulators refuse to allow OBES to raise their prices to offset the costs of financing this defensive posture proposed by robustness. Regulators are concerned with the potential consumer backlash for raising service rates to bolster BES defenses against cyber-attackers. Thus, policymakers must create legislation to incentivize CIOs to invest in increasing resilience without placing the financial burden on the consumer. One approach is to award FEMA grants generally given to public authorities to private CIOs to improve the resilience of their critical infrastructure. Congress can also create legislation to encourage private investors to invest in local and state critical infrastructure. Such measures will ensure that CIOs cannot raise their rates to a level that is unsustainable for the consumer, thereby

[86] Obama. *Executive Order: Improving Critical Infrastructure Cybersecurity.*

abiding by pricing standards set by their regulators. Nevertheless, policymakers should also consider allowing CIOs to raise their fees to finance the implementation of robustness in their critical infrastructure. Although this may conflict with the interests of regulators, the U.S. government can create regulation to protect the consumer while bolstering robustness. One example is to mandate that all revenue generated by a price increase must be allocated to building resiliency. Ultimately, policymakers must take action to solve the economic cost and regulatory issues of building expensive layered defense and redundancy that presently serves as a limitation for robust cyber deterrence.[87]

Even with a modest increase in revenue, CIOs will not be able to completely secure their critical infrastructure from cyber-attacks. With this in mind, a more cost-effective method to bolster the resiliency of U.S. critical infrastructure is to take a holistic approach to implementing the new USCDS based on robustness. CIOs must maximize their limited resources and invest enough into the robustness strategy to absorb the effects of a cyber-attack without sacrificing their ability to function as an enterprise. OBES should development assessment criteria to identify the most vulnerable segments of U.S. critical infrastructure that require additional layers of defense and redundancy. For example, OBES should identify which of their critical infrastructure can withstand a cyber-attack without degradation of service and those that will create a disruption. Operators of critical infrastructure must also prioritize the most critical of systems within their geographic area to more effectively decide how to allocate their limited resources. Without additional revenue to finance robustness, CIOs must resort to these holistic

[87] Moteff. *Critical Infrastructure Resilience.*

measures in order to adequately bolster the resiliency of their critical infrastructure without exhausting their finite resources. Protecting essential functions rather than the critical infrastructure in its entirety will still add additional defensive layers and redundancy required to effectively deter cyber-attackers through the new USCDS. Furthermore, a holistic financial approach can allow CIOs to circumvent the economic costs of resiliency in order to make the new USCDS based on robustness more effective.[88]

Ultimately, the success of the new USCDS based on robustness depends on the strength of a public-private sector partnership (PPP). PPPs are symbiotic relationships with the public sector dependent upon the success of private companies to stimulate the economy, whereas the public sector provides the security necessary for the survivability of the private sector. While the federal government serves multiple customers and missions, sharing intelligence with CIOs does not receive high priority.[89] The public sector must increase their collaboration with CIOs to improve efforts to protect critical infrastructure in the absence of formal regulatory policies. The Obama Administration's *Executive Order for Improving Critical Infrastructure Cybersecurity* is a positive step towards greater collaboration due to its recommendation to enhance the sharing of information related to critical infrastructure protection. However, federal, state, and local governments must take steps to further the public-private sector partnership by

[88] Egli, Dane S. *Beyond the Storms: Strengthening Security & Resilience in the 21st Century*. Laurel, MD: Johns Hopkins University Applied Physics Laboratory (JHU/APL), 2013.

[89] U.S. Department of Homeland Security. National Infrastructure Advisory Council. *Intelligence Information Sharing: Final Report and Recommendations*. 2012. Accessed July 13, 2013. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

incentivizing CIOs to make their critical infrastructure more robust in accordance with the new USCDS. For example, the public sector can offer subsidies or grants to collaborating CIOs willing to bolster their security. Likewise, CIOs must also improve collaborative efforts with their public sector partners by reducing their resistance to forming public-private sector partnerships. CIOs fear public-private sector partnerships may provide their competitors with a market advantage that may threaten their stream of revenue. The new USCDS based on robustness can only be achieved if public and private sector stakeholders in critical infrastructure are willing to partner on measures to improve resiliency.[90]

With CIOs able to increase revenue and federal regulation mandating an increase in cyber defense, the proposed cyber strategy of robustness can address the outstanding criteria limiting its effectiveness. Passing legislation to raise revenue, incentivize private investors, or allocate FEMA grants to CIOs is the most effective approach to addressing the issues of economic costs and regulation in a new USCDS based on robustness. However, this solution is only attainable if the U.S. government can create policies promoting such revenue-raising measures. Given the uncertain timeframe of creating these policies, this recommendation is a long-term solution to an immediate issue to securing critical infrastructure. Although public-private sector partnerships can provide a short-term solution to defending critical infrastructure, the distrustful culture of private CIOs makes the challenge of strengthening public-private sector partnerships difficult to achieve. As a result, the best short-term approach to building resiliency in U.S. critical

[90] Ibid.

infrastructure in accordance with robustness is to adopt a holistic approach. This allows CIOs to circumvent the issues of economic costs and regulation that limit the effectiveness of robustness. This measure will also allow CIOs to identify their vulnerabilities and efficiently allocate their limited resources to build layered defenses and redundancy for the most critical and vulnerable of their systems.

Having all CIOs develop layered defenses and infrastructure redundancy, this new USCDS will better position CIOs to absorb attacks and collect information on their aggressors. Solving the regulation and economic cost issues also enhances the option of tailoring a response to the specific threat. Ensuring all CIOs are robust enough to absorb attacks also ensures that CIOs will have the ability to collect information that can be used to respond against the cyber-attacker at the most opportune time. Based on the shortfalls of the Obama Administration's current cyber deterrence strategy, the new strategy is in a better position to protect the United States from dangers posed by state and non-state cyber-attackers. The U.S. was not wrong when it tried to recycle Cold War deterrence strategies for use in cyberspace. However, the Obama Administration's current strategy is merely incomplete and lacks a critical component. This component is the difference between the current strategy and a new U.S. deterrence strategy that includes robustness; the use of objective denial with defense-in-depth and redundancy to withstand attacks and improve the ability to punish attackers for striking critical infrastructure through cyberspace. Only by implementing this critical component will U.S. cyber deterrence be complete and effective in deterring America's enemies. Critical infrastructure owners can holistically work to make their systems more robust to a cyber-attack in the short-term;

however they must receive the necessary financial support through government aid or increased service to effectively bolster their defenses in the long-term.

Bibliography

Albanesius, Chloe. "Anonymous Takes Down CIA Web Site." PCMAG. Last modified February 10, 2012. http://www.pcmag.com/article2/0,2817,2400140,00.asp.

Andres, Richard B. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.

Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." Accessed May 15, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Armending, Taylor. "Security Experts Push Back at 'Cyber Pearl Harbor' Warning." CSO. Last modified November 7, 2012. http://www.csoonline.com/article/720930/security-experts-push-back-at-cyber-pearl-harbor-warning.

Arquilla, John. *Worst Enemy: The Reluctant Transformation of the American Military*, 129. Chicago: Ivan R. Dee, 2008.

Art, Robert J. "To What Ends Military Power?" *International Security* 4, no. 4 (1980): 3-35.

Brown, Chris. "Phases of a Cyber-attack / Cyber-Recon." United States Naval Academy. Accessed July 17, 2013. http://www.usna.edu/CS/si110arch/si110AY12F/lec/l32/lec.html.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S."*The New York Times*, October 11, 2012. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

Burgess, James. "Chinese Military Renews Cyber-Attacks, Focusing on US Electrical Grid." Oil Prices & Energy News: Crude Oil Price Charts, Investment Advice. Last modified May 23, 2013. http://oilprice.com/Latest-Energy-News/World-News/Chinese-Military-Renews-Cyber-Attacks-Focusing-on-US-Electrical-Grid.html.

Burns, Bryan, Dave Killion, Nicolas Beauchesne, Eric Moret, Julien Sobrier, Michael Lynn, Eric Markham, et al. *Security Power Tools*, 421-430. Sebastopol, CA: O'Reilly, 2007.

Cooper, Jeffrey R. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 106-114. Washington, DC: Georgetown University Press, 2012.

Egli, Dane S. *Beyond the Storms: Strengthening Security & Resilience in the 21st Century*. Laurel, MD: Johns Hopkins University Applied Physics Laboratory (JHU/APL), 2013.

Frederick, Erwin E. *Testing A Low-Interaction Honeypot Against Live Cyberattackers*. 2011 n.d. Accessed March 15, 2013. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA552206&Location=U2&doc=GetTRDoc.pdf.

Goodman, Will. "Cyber Deterrence: Tougher In Theory Than In Practice?" *Strategic Studies Quarterly* 4, no. 3 (2010): 102. Accessed January 15, 2013. http://0-go.galegroup.com.bianca.penlib.du.edu/ps/retrieve.do?sgHitCountType=None&sort=DA-SORT&inPS=true&prodId=AONE&userGroupName=udenver&tabID=T002&searchId=R1&resultListType=RESULT_LIST&contentSegment=&searchType=AdvancedSearchForm¤tPosition=1&contentSet=GALE%7CA243958196&&docId=GALE|A243958196&docType=GALE&role=.

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. "Leaving Deterrence Behind: WarFighting and National Cybersecurity." *Journal of Homeland Security and Emergency Management* 7, no. 1 (2010): 17. doi:10.2202/1547-7355.1636.

Libicki, Martin C. "Cyber Deterrence and Cyberwar." RAND Corporation. Last modified 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Lowther, Adam. *Deterrence Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century*, 165-166. New York, NY: Palgrave Macmillan, 2012.

Lynn, William, III. "Defending A New Domain." *Foreign Affairs* 89, no. 5 (2010): 99-100. http://www.usna.edu/AcResearch/NASEC2012/William_Lynn_III_Defending_a_New_Domain.pdf.

Morgan, Patrick M. *Deterrence Now*, 8. Cambridge [England]: Cambridge University Press, 2003.

Moteff, John D. *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*. Congressional Research Service, 2012. Accessed April 28, 2013. http://www.fas.org/sgp/crs/homesec/R42683.pdf.

Obama, Barack H. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Executive Office of the President of the United States, 2009. Accessed March 15, 2013. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Obama, Barack H. *Executive Order: Improving Critical Infrastructure Cybersecurity*. Executive Office of the President of the United States, Office of the Press Secretary, 2013. Accessed March 14, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Obama, Barack H. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Executive Office of the President of the United States, 2011. Accessed March 15, 2013. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Overman, Thomas M., Terry L. Davis, and Ronald W. Sackman. "High Assurance Smart Grid." Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. Last modified 2010. http://0-delivery.acm.org.bianca.penlib.du.edu/10.1145/1860000/1852734/a61-overman.pdf?ip=130.253.4.14&id=1852734&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1E66739E26778C50D1A135E9E0C10ED60&CFID=234176311&CFTOKEN=63291536&__acm__=1374080167_a9efbb782636cad50c2f401490e3a2b4.

Pape, Robert A. *Bombing to Win: Air Power and Coercion in War*, 4-6. Ithaca, N.Y.: Cornell University Press, 1996.

Sanger, David E., and Eric Schmitt. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure." *The New York Times*, July 26, 2012. http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=0.

Singer, Peter W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*, 184-186. New York: Penguin Press, 2009.

Smith, Randy F. "Defense in Depth." *Windows IT Security* 5, no. 11 (2005): Accessed May 3, 2013. http://0-search.proquest.com.bianca.penlib.du.edu/docview/215123642.

Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (2012): 148-170. doi:10.1080/13523260.2012.659597.

Stevenson, Angus, and Christine A. Lindberg. *New Oxford American Dictionary*. Oxford: Oxford University Press, 2010.

Thomas, Troy S. "Beyond Pain: Coercing Violent Non-State Actors." Last modified 2010. http://www.usafa.edu/df/inss/Research Papers/2010/Thomas Coercing VNSA.pdf.

U.S. Department of Defense. *Department of Defense Dictionary Of Military and Associated Terms*. Ft. Belvoir: Defense Technical Information Center, 2010. Accessed July 15, 2013. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

U.S. Department of Energy and the North American Electric Reliability Corporation. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System: A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop*. 2010. Accessed February 17, 2013. http://www.nerc.com/files/HILF.pdf.

U.S. Department of Energy. Federal Energy Regulatory Comission. *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. 2013. Accessed July 15, 2013. http://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf.

U.S. Department of Energy. Federal Energy Regulatory Commission. *Assessment of Demand Response & Advanced Metering*. 2008. Accessed July 15, 2013. http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf.

U.S. Department of Energy. Office of Electric Delivery and Energy Reliability. *Smart Grid*. n.d. Accessed July 15, 2013. http://energy.gov/oe/technology-development/smart-grid.

U.S. Department of Energy. *Roadmap To Achieve Energy Delivery Systems Cybersecurity*. 2011. Accessed May 20, 2013. http://energy.gov/sites/prod/files/Energy Delivery Systems Cybersecurity Roadmap_finalweb.pdf.

U.S. Department of Homeland Security. National Communications System. *Technical Information Bulletin 04-1*. 2004. Accessed July 15, 2013. http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf.

U.S. Department of Homeland Security. National Cyber Security Division. *Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-In-Depth Strategies*. 2009. Accessed May 1, 2013. http://ics-cert.us-cert.gov/practices/documents/Defense_in_Depth_Oct09.pdf.

U.S. Department of Homeland Security. National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations*. 2009. Accessed July 14, 2013. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

U.S. Department of Homeland Security. National Infrastructure Advisory Council. *Intelligence Information Sharing: Final Report and Recommendations*. 2012. Accessed July 13, 2013. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

U.S. Department of Homeland Security. *Malware Infections In The Control Environment*. ICS-CERT Monitor, 2012. Accessed April 2, 2013. http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf.

Glossary

Attribution: The ability to accurately identify a perpetrator behind an attack.

Bulk Electric System (BES): The collective elements of U.S. infrastructure for the operating, generating, and/or transmitting electricity at 100 kilovolts (kV).[91]

Computer Network Attack (CNA): Actions taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[92]

Contestability: The ability for an accused aggressor to contest the attribution of attack without punishment from the target.

Critical Infrastructure Operator (CIO): The public and/or private sector owners of critical infrastructure within the United States.

Defense: The use of force to repel an attack or to prevent an attack from making further progress and/or mitigate damage if attacked.[93]

Defense-in-Depth: The act of implementing multiple layers of defense in order to weaken, exploit, and/or deter the aggressor.

Deterrence: Coercing aggressive actors, whether with the threat of force or by denying their objectives, from attacking or undertaking a negative action. Three types of deterrence are important to this study:

---

[91] U.S. Department of Energy. Federal Energy Regulatory Comission. *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. 2013. Accessed July 15, 2013. http://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf.

[92] U.S. Department of Defense. *Department of Defense Dictionary Of Military and Associated Terms*. Ft. Belvoir: Defense Technical Information Center, 2010. Accessed July 15, 2013. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[93] Art. "To What Ends Military Power?" 5.

- **Denial Deterrence**: Deterring aggressive actors by denying their ability to achieve their strategic objectives, thereby undermining the enemy to the point where it begins to doubt its own strategy and thus does not engage in hostilities.
- **Punitive Deterrence**: Deterring aggressive actors by threatening to respond with force against their valued interests or the aggressor itself in the event of an attack against the state.
- **Cyber Deterrence**: Coercing aggressive actors from attacking the state via cyberspace, whether through denial and punishment, and maintaining their deterred behavior.

Public-Private Sector Partnership (PPP): While the term is commonly used for any formal arrangement between the private sector and government to address and/or coordinate a shared area of responsibility, in the context of this research, it refers to a symbiotic relationship between public and private sector stakeholders over the administration, maintenance, and security of critical infrastructure in the United States.

Redundancy: Implementing additional infrastructure components to ensure the survivability, or continuity of service, of the system should other components fail.[94]

Regulators: Public and/or private sector organizations that oversee the administration, maintenance, and security of critical infrastructure in the United States.

Remote Terminal Unit (RTU): Components of the Bulk Electrical System (BES – see above) that transmit information to supervisory control and data acquisition (SCADA – see below) systems.

Resilience: The ability for critical infrastructure to reduce the duration and/or magnitude of a computer network or physical attack.[95]

Robustness: Fortifying critical infrastructure to absorb Computer Network Attacks (CNA – see above), ensure continuity of service, and deny the attacker's objectives.

Scalability: The extent to which a state can retaliate against an attack without violating the Just War Tradition.

---

[94] Stevenson, Angus, and Christine A. Lindberg. *New Oxford American Dictionary*. Oxford: Oxford University Press, 2010.

[95] U.S. Department of Homeland Security. National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations*. 2009. Accessed July 14, 2013. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

Smart Grid: Electric grids that use information and communications technology to regulate the production and distribution of electricity.[96]

Smart Meters: Electrical meters that process data on energy consumption while relaying information back to the utility for monitoring and billing purposes.[97]

Spy-VS-Treaty: The resistance by states to allow other states access to their network for investigative purposes, despite formalized agreements, due to cybersecurity threats.

Supervisory Control and Data Acquisition (SCADA): Systems used to monitor and control equipment within the Bulk Electrical System (BES – see above).[98]

Synchrophasors: Technology used to monitor in real-time to detect disturbances, predict instability, and control the problem.

Tailored Response: Using information collected from an attributed CNA to design a response against the aggressor at the most opportune moment. A tailored response can also be used to deny and deter potential aggressors.

[96] U U.S. Department of Energy. Office of Electric Delivery and Energy Reliability. *Smart Grid*. n.d. Accessed July 15, 2013. http://energy.gov/oe/technology-development/smart-grid

[97] U.S. Department of Energy. Federal Energy Regulatory Commission. *Assessment of Demand Response & Advanced Metering*. 2008. Accessed July 15, 2013. http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf.

[98] U.S. Department of Homeland Security. National Communications System. *Technical Information Bulletin 04-1*. 2004. Accessed July 15, 2013. htt://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf.