SAND2016-1373R

HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Final Draft – 2nd submission (30 May 2015)

ANALYTIC FRAMEWORK FOR UNITED STATES CYBER DETERRENCE STRATEGY

Heather Blackwell, Lt Col, United States Air Force

Chrisma Jackson, Sandia National Laboratories

Jennifer McCann, Office of the Director for National Intelligence / National Counterterrorism Center

Harvard University

John F. Kennedy School of Government

National Security Program

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

The views expressed in this academic research paper are those of the authors and do not reflect the official policy or position of Harvard University, the U.S. government, or the Department of Defense.

ACKNOWLEDGEMENTS

The authors would like to thank the following people critical to the development of this document: Dr. Graham T. Allison, Jr., W. Eric Herr, Dr. Martin Feldstein, Mimi Goss, James Gosler, Michael M. Johnson, Lt Gen Tad Oelstrom (ret.), Dr. Joe Nye, Dr. James Peery, Bruce Schneier, Admiral William Studeman, (ret.), Dr. James H. Waldo, and Jean Woodward.

Thank you for your guidance, critical review, and/or feedback in the development of this paper and for your insights into the subject of cyber security and deterrence.

Table of Contents

Executive Summary 2
Chapter 1: Why Cyber Deterrence Strategy is Needed 4
Chapter 2: What U.S. Cyber Deterrence Strategy Should Include 8
Chapter 3: How Cyber Deterrence Should Be Implemented 18
Chapter 4: An Example of Cyber Deterrence Strategy Implementation 28
Chapter 5: Proposed U.S. Cyber Deterrence Strategy Implementation Memo 32
Summary and Recommendations 38
Appendix: Proposed Cyber Deterrence Strategy Options Memo 40
End Notes 44
Bibliography 47

List of Figures

Figure 1: Cyber Deterrence Analytic Framework

Figure 2: Analytic Framework with "Uses of Cyberspace" Axis

Figure 3: U.S. Internet Use, 1995 – 2014

Figure 4: Analytic Framework Application: Sony Pictures

Table: Key Cyber Threats

Executive Summary

If the United States (U.S.) government allows cyberattacks to continue on their current trajectory of increased frequency and effect, the bonds holding our society together will be jeopardized, potentially impacting the survival of our society as we know it.[1] Actions must be taken not only to defend against, but also to deter future cyberattacks. To achieve a credible and actionable U.S. Cyber Deterrence Strategy, the following three lines of effort are recommended for implementation by the White House:

1. Add a sixth priority to the Obama Administration's current cyberspace priorities to state: "Advance our cyber response policies and capabilities to further protect the country's national interests by deterring attacks within cyberspace."
2. Adopt the proposed Cyber Deterrence Analytic Framework as a guide for policy makers to use when determining the appropriate response to a cyberattack.
3. Implement the proposed Presidential Policy Directive outlining the United States' deterrence policy for cyber.

These recommendations for establishing a U.S. Cyber Deterrence Strategy address the following key findings:

- As the U.S. private sector owns and operates over 90% of all of the networks and infrastructure of cyberspace,[2] an effective policy must be communicated clearly across the government, business enterprise, and most importantly, to the people.
- More so than any time in our nation's history, individuals, companies, and organizations depend on cyberspace for uses ranging from social interactions to sustaining democracy.
- Threats existing within the cyber domain have grown both in attack vector complexity and societal impact.
- The current Presidential Executive Orders and Policy Directives related to cyber deterrence **do not** include a strategy for deterring attacks.

The concepts presented in this paper were derived from interviews with experts in subjects ranging from deterrence philosophy, nuclear weapons implementation, U.S. cyber operations,

and U.S. cyber policy. In addition, theories on deterrence strategies are explored, ranging from the 1960s to present to develop a deterrence strategy unique to cyber. Lastly, recent examples of cyberattacks are examined to provide evidence for the need to establish consequences for those individuals or countries that continue to behave nefariously within cyberspace. To form a strong foundation for a U.S. Cyber Deterrence Strategy, the U.S. must establish and clearly articulate the consequences for nations or individuals if they choose to initiate a cyberattack on the U.S. or its national interests.

Chapter 1: Why Cyber Deterrence Strategy is Needed

"If you look at an [cyber] attacker's expected benefit and expected risk, the equation is pretty good for them. Nothing is going to change until we can get their expected net gain close to zero or — God willing — in the negative."

Howard Shrobe, computer scientist at Massachusetts Institute of Technology[3]

To push a cyber attacker's expected gain to zero requires the United States to add consequences to the equation of a cyberattack. Therefore, it is critical the U.S. clearly defines the consequences of an attack so would-be attackers modify their behavior so as to not attack in the first place. To define consequences of a cyberattack, a U.S. cyber deterrence strategy is proposed with two fundamental components:

- An analytic framework to guide policy making and implementation
- A U.S. policy in the form of a draft Presidential Policy Directive (PPD) to articulate how the U.S. will respond to the assailant when attacked in cyberspace

The broad definition of deterrence includes **anything that actually serves to deter an actor from nefarious behavior**.[4]

"A cyberattack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11."[5]

Secretary of Defense Leon Panetta, 2012

In December 2014, the cyber-based attack followed by threats of "9/11 style attacks"[6] forced Sony Pictures Entertainment, an American-based subsidiary of Japanese multinational Sony Corporation, to halt operations and persuaded them to modify the release of "The Interview." This attack, along with the threats, and the outcomes changed how people view the battle that continues to escalate within cyberspace.

Due to the United States' proactive efforts, it has not had another terrorist attack on the homeland since 9/11. Yet, using lessons learned about protecting national interests, the U.S. has taken few visible concrete steps to thwart threats against another major aspect of U.S. national security: cyberspace.

Multifarious threats within cyberspace are increasing both in quantity and severity. Trends in cyberattacks show an increase of:[7]

- 10,000-fold in new digital threats in the past 12 years
- 62% in cyberattacks over the past year

Cyberattacks, as Chapter 3 will discuss, are exploiting an environment based on sharing and innovation, not security. These attacks are not only increasing in number, but also in complexity and scope. For example, The New York Times reports that in the last two years, "the White House, the State Department, the top federal intelligence agency, the largest American bank, the top hospital operator, energy companies, retailers and even the Postal Service" have been targets of successful cyberattacks.[8]

In his testimony before the Senate Homeland Security Committee in late 2013, FBI Director James B. Comey said that "the risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States." Supporting this statement, the PEW Research Center reports that Americans rank "Cyber Attacks from Other Countries" as the number two security concern immediately behind the "Threat of Islamic Extremist Groups."[9]

With the data showing the **number** of cyberattacks increasing, **threats** to the U.S. national security is increasing, and the **American public is more concerned** with cyberattacks, it would seem logical that the government would take concrete steps to thwart cyber threats to U.S. national security. Concrete steps, however, are not easy to take when it comes to cyberspace. The Congressional Research Service recently reported, "no major cybersecurity legislation has been enacted since 2002."[10] [1] Moreover, NATO is discussing cyber, with a focus on defense and

[1] At present two House bills are pending in the Senate (H.R. 1560, "Protecting Cyber Networks Act," and H.R. 1731, "National Cybersecurity Protection Advancement Act"). Additionally, on 1 April 2015 the President signed an Executive Order that would levy financial sanctions against malicious overseas actors that stand to profit or otherwise benefit from cyber-related activities targeted against the United States.

alliance support.[11] Currently, the most significant public knowledge of U.S. cyberspace activities is derived from leaked documents from Edward Snowden, former National Security Agency contract employee.

Beyond efforts already underway to defend assets within the cyber infrastructure, the U.S. should thwart cyberattacks through deterrence. The objective of deterrence is to convince the prospective adversary it is not in their best interest to launch a cyberattack against U.S. assets, as the consequences will be too great. Developing such a cyber-deterrence strategy, however, faces both technical and philosophical impediments.

Research shows that a national policy on cyber faces the following hurdles to development and implementation:

- Cyber technology changes faster than policy can respond
- Cyber architecture has made the world so entangled that changes in one country can have drastic impacts on many other countries[12]
- Cyberspace includes military, multi-national businesses, and individuals
- Cyber operations to protect and defend assets and individuals in cyberspace require involvement from multiple U.S. agencies
- Cyberspace requires strategic thinking for a technical, if not esoteric, problem
- Cyberspace leadership is believed to be in the hands of the U.S.[13]

In addition to the difficulties of establishing a national policy on cyber, many nuclear deterrence experts and cyber experts believe cyber deterrence is impractical because it is:

- Difficult, if not impossible, to assign attribution to the cyber-attacker[14]
- Difficult to deter a non-state actor[15]
- Difficult to articulate a clear deterrence strategy without weakening the ambiguity.[16] Ambiguity is the actual deterrent.

Attribution is difficult. The ability to attribute an attack to a defined actor and associate the actor to a cause/state should not be trivialized, but the difficulty in solving the attribution problem is the most popular argument against developing a deterrence model. However, the ability to assign attribution to an attack is becoming more of a reality via integrated technical

forensics and intelligence and this proceeding forward with the development and communication of a deterrence model in parallel with the continued development and refinement of attribution is essential.[17] Discussions and arguments about cyber attribution can paralyze the process of outlining the U.S. response to a cyberattack. As an establishment of precedence, it is important to note that the U.S. nuclear deterrence strategy was developed in absence of absolute certainty. In Cyber Power and National Security, Richard Kugler "During the Cold War, the United States possessed enough evidence of the Soviet Union's *potential* uses of military forces in a war to justify…the creation of a deterrent strategy."[18]

It is impossible to deter a non-rational actor. In other words, an actor can remain anonymous and has no fear of consequences. This is a much generalized argument and does not give credit to the range of 'actors' within cyberspace who can be deterred to include cyber criminals and state-sponsored cyber armies. On 26 February 2015, Russia, China, Iran, and North Korea were listed as the top nation-state cyber threats; these are entities that can be deterred if the U.S. has a strategy in place.[19]

Ambiguity is the deterrent. The third argument against codifying a national deterrence strategy is that having **ambiguity** in how the U.S. will respond actually **deters the enemy** because when the enemy is uncertain, they must pause before considering an attack on the U.S.[20] The problem with this argument is that deterrence will not work if your adversary does not know how you will respond to an attack. Harvard Professor Graham Allison, a U.S. expert on nuclear deterrence, succinctly described proper employment of deterrence in his book Nuclear Terrorism: "…even during the most dangerous moments of the Cold War, a nation that attacked the United States with a nuclear-armed ballistic missile would **know** that it had signed its own death certificate, since U.S. retaliation would be immediate and overwhelming."[21] That is exactly what a cyber deterrence strategy is aiming to do: make it perfectly clear to anyone who launches a cyberattack against the U.S. to expect a response.

Chapter 2: What U.S. Cyber Deterrence Strategy Should Include

"Thus far, the United States has not been noticeably forceful in stating its intentions to deter major cyberattacks and, if necessary, to respond to them with decisive force employing multiple instruments of power"[22]

Richard L. Kugler, Cyberpower and National Security

In his 1966 book, Arms and Influence, Thomas Schelling described the conditions similar to what would happen in a serious cyberattack including the potential to be catastrophic and rapid: "To compress a catastrophic war within the span of time that a man can stay awake drastically changes the politics of war, the process of decision, the possibility of central control and restraint, and the motivations of people in charge."[23]

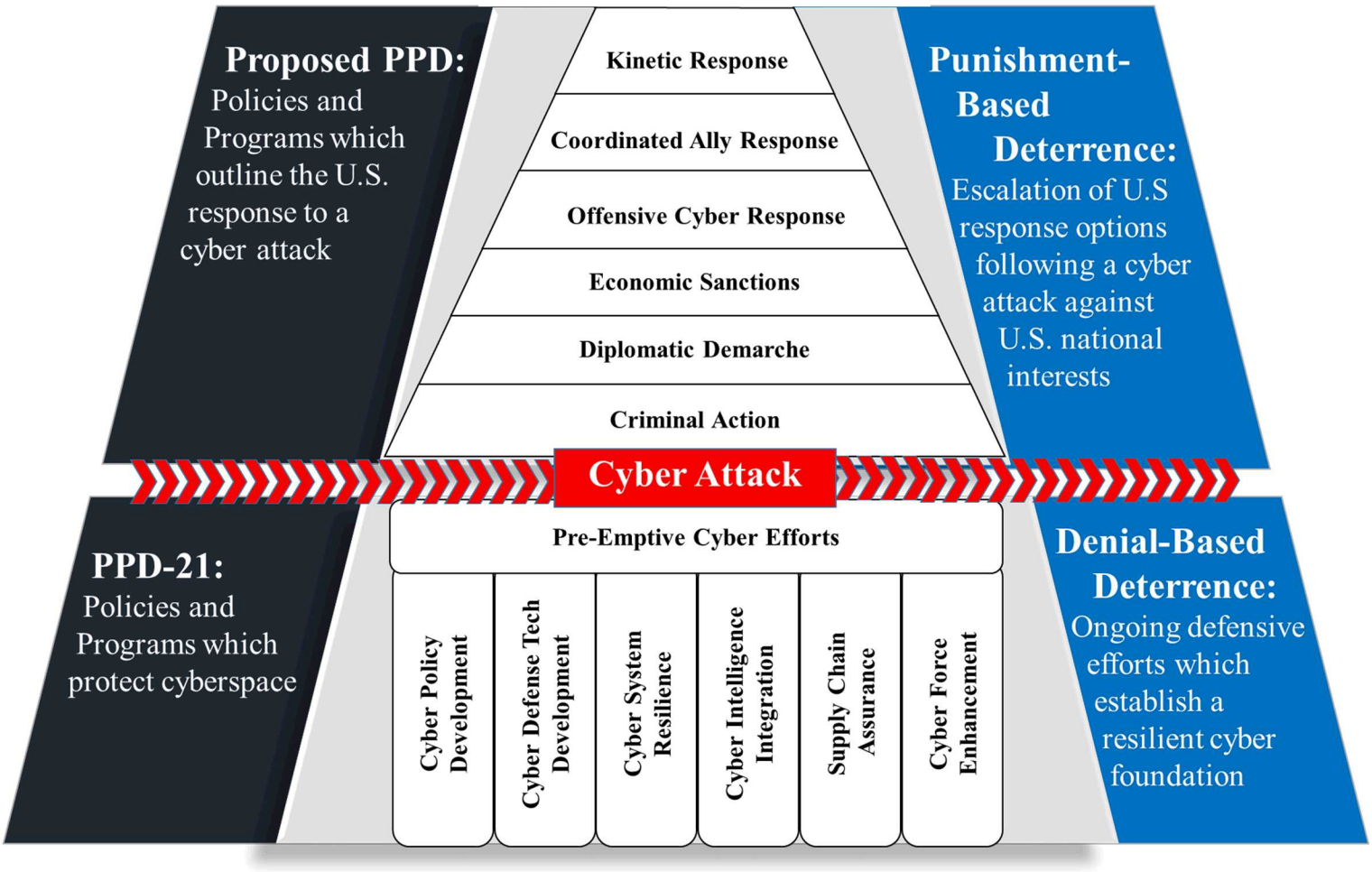
A cyber deterrence strategy with clearly defined actions would not only deter adversaries, but provide decision makers with a frame of reference to be used in the midst of a cyberattack. This chapter introduces the analytic framework component of the cyber deterrence strategy, which serves to "forcefully state" the U.S. intentions in responding to a cyberattack. Chapter 5 details the policy component of the cyber deterrence strategy is derived from the analytical framework.

The framework, shown in Figure 1, seeks to protect the rights of citizens and businesses, but also clearly a would-be adversary how the U.S. defends against and will respond to cyberattacks using all instruments of national power to include political, diplomatic, economic, and military. This framework is simple: build a sound cyber defense and if attacked, escalate through the options as dictated by impact of the attack.

The actions listed in Figure 1 illustrate a graduated escalation response to a cyberattack. An effective deterrence strategy requires three elements:

- **Clarity** of line the enemy cannot cross
- **Capability** to respond and impose costs that exceed the enemy's benefits of attacking
- **Credibility** that you will do it [24]

FIGURE 1 CYBER DETERRENCE ANALYTIC FRAMEWORK



The development of cyber norms by the U.S. government provides the **clarity** of the line the enemy cannot cross. The framework provided herein suggests a structural reference for use by U.S. policymakers in the midst of a crisis, and it communicates U.S. response **(capability)** to the international community– a key aspect of deterrence.

Denial-Based Deterrence

The proposed cyber deterrence analytic framework advocates for two types of deterrence: denial-based and punishment-based.[25] Denial-based deterrence exists in the bottom portion of the framework where there is ongoing cyber defensive efforts. Denial-based deterrence could arguably be the most important type of deterrence because in cyber, as in other domains, if one can make defenses so strong that the cost for the would-be attacker to overcome them is too high,

the attacker is deterred and there is no need to move up the escalation options. The following describe the framework's denial-based deterrence components moving from left to right.

Cyber Policy Development

A key component of denial-based deterrence is ensuring strong relationships and clear policies and procedures exist between businesses and the government with respect to preparation for and response to cyberattacks. Cyber attackers will think twice about hacking a company when they realize the U.S. will levy its intelligence and cyber capabilities of both the business and government to identify and hold the attacker accountable. In addition, cyber companies will be less likely to take on the attackers themselves if they know the U.S. government will defend them in the face of a nation state infrastructure attack.

Cyber Defense Technology Development and Insertion

Government and industry have made great strides toward security improvements for cyber defense, but must continue to evolve technologies to find cost effective integration solutions commensurate with the evolving threats. Activities strengthening cyber defense posture include:

- Development of security standards via industry initiatives (e.g. Trusted Computing Group)
- Extensive work on Trust and Network Defense at DARPA
- Implementation of EINSTEIN 3 on government Networks and EINSTEIN on defense contractor networks).[26]

These technologies have provided some improvement by providing network intrusion detection and improved defenses on government networks, but concerns about cost and privacy issues have thwarted increased adoption of technology by government and industry. In particular the adoption of security technology has not yet been fully realized as the reported cost of intrusions are still be reported as "…not material".[27]

Cyber System Resilience

One key defensive measure employed across systems is resiliency. Presidential Decision Directive/PDD-21 defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to

withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents".[28] Prioritizing which projects and programs to retain or restore immediately following an attack is critical to enhancing cyber resiliency to attack. Diversity or redundancy of systems, both software and hardware, is now vital because of the increased complexity of the methods cyber attackers employ. Enhancing cyber resilience was a key theme in the execution of President Obama's executive order intent on improving critical cybersecurity infrastructure.[29]

Cyber Intelligence Integration

As attacks become increasingly sophisticated, integrated intelligence capability with technical forensics is increasing in value. The FBI has noted many successes nationally and internationally in the collection and dissemination of intelligence data, both unclassified and classified.[30] The role of the soon-to-be-established Cyber Threat Intelligence Integration Center (CTIIC) within the Office of the Director of National Intelligence (ODNI), as outlined in H.R. Bill 1560 "Protecting Cyber Networks Act,"[31] will aim to ensure cyber-related intelligence is shared and coordinated across relevant USG agencies. "[CTIIC] will be a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests…and assist relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats."[32]

> Deployment of security intelligence systems makes a difference. The cost of cybercrime is moderated by the use of security intelligence systems. Findings suggest companies using security intelligence technologies were more efficient in detecting and containing cyberattacks. As a result, these companies enjoyed an average cost savings of nearly $4 million when compared to companies not deploying security intelligence technologies.[33]

Supply Chain Assurance for Information System Components

Protection of the sources of cyber equipment for critical U.S. government applications has become an important aspect of denial-based deterrence. Guidance and direction for supply chain protection is now documented in DoD and National Institute of Standards and Technology (NIST) publications, as well as rules excluding contractors based on supply chain risks.[34]

For example, the DoD acquisition process now utilizes Program Protection Plans (PPPs) to protect both the technology and the information associated with the acquisition program.

Reinforcing the need for supply chain assurance, the DoD's Acquisition Guidebook defines PPPs as a method to: "mitigate the risk that the technology will be lost to an adversary; where the capability is derived from integration of commercially available or developed components, Program Protection mitigates the risk that design vulnerabilities or supply chains will be exploited to degrade system performance."[35]

The PPP process is a first step toward understanding the security needs and implementing solutions, but the PPP is documentation of implemented security that depends on development of affordable, scalable solutions that thwart nation state threats for the Defense Program Internet of Things. Supply chain assurance is increasingly difficult as an increasing number of microelectronics are made offshore and/or in foundries owned by non-U.S. investors.[36] PPP analyzes the supply chain and based on the threat suggests cost-effective administrative and technical solutions to mitigate the threats.

In 2015, the Pentagon made additional concrete steps into making cybersecurity an integrated part of the acquisition process. In January 2015, the Joint Chiefs of Staff (JSC) "included cybersecurity under the survivability key performance parameter with the acquisition of new defense technologies with embedded computing systems."[37] Following on the JSC statement, Frank Kendall, Under Secretary of Defense for Acquisition, Technology and Logistics, announced "plans to add cybersecurity to the next phase of his better buying power initiative, and was also working on a special section on cybersecurity requirements to be added to the Pentagon's guidelines for buying weapons."

Supply chain and acquisition efforts are still in their infancy and evolving quickly. The effectiveness and implementation of the efforts are still to be determined.

Robust Cyber Forces

As both civilian and military organizations are attacked, many have discussed the subject of Active Defenses or "Hacking Back" at the adversary. From the civilian sector, liability and escalation issues as well as legal issues surface, dissuading the civilian sector from engaging in active defense measures and the development of offensive cyber teams independent of government.

According to Navy Admiral Mike Rogers, Commander of U.S. Cyber Command (CYBERCOM), the creation of the organization acknowledged the increasing importance of the cyber domain in warfare by developing an organization: 1) capable of protecting and defending DoD networks, provide a broader range of options to operational commanders and policy makers and, 2) defend the nation against the potential of nation-states, groups and individuals to conduct offensive cyber activities against critical U.S. infrastructure.[38] The creation of CYBERCOM provides a long-term plan to develop robust cyber forces to support the cyber defense posture.

Development, exercising and integrating these forces in to the larger structure is crucial. Efforts such as joint cyber war games with the United Kingdom[39] are a first start, but further development and exhibition of the credible capability is key to this module of the deterrence.

Pre-Emptive Cyber Efforts

The rung of the framework's ladder that ties the denial-based deterrent efforts with punishment-based deterrence options is the employment of pre-emptive cyber operations. If the U.S. has intelligence that a nation state or terrorist organization is supporting or harboring cyber attackers or cyber attacking capabilities within their borders, the U.S. must be prepared to take pre-emptive measures to ensure those attackers or weapons are not used on U.S. assets.

The FBI has been successful in working internationally on the defensive side of pre-emptive cyber efforts. One example the FBI highlighted was their work in the disruption of botnets:

> One area in which we recently have had great success with our overseas partners is in targeting infrastructure we believe has been used in distributed denial of service (DDoS) attacks, and preventing that infrastructure from being used for future attacks. A DDoS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network. Since October 2012, the FBI and the Department of Homeland Security (DHS) have released nearly 168,000 Internet Protocol addresses of computers that were believed to be infected with DDoS malware. These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDoS attacks.[40]

Pre-emptive measures will be increasingly vital in deterring attacks as well as reducing the consequences associated with attacks. As intelligence information and mechanisms of communication improve, this will be an increasingly valuable form of protection for cyberspace.

Punishment-Based Deterrence

Although defending against an assault and making someone afraid to take something from you are different,[41] policy makers should address both approaches. The denial-based portion of the framework discussed is addressed in PPD-21.

The escalation options of the framework are the basis for the proposed PPD (Chapter 5) and describe punishment-based deterrence. Threat of damage, or punishment-based deterrence, compels actors to modify their behavior.[42] However, this type of deterrence still leaves the choice to attack in the hands of the assailant.[43] Therefore, it is the coordinated use of both the denial-based and punishment-based approaches included in the framework, which will lead to the success of a deterrence strategy. The framework's punishment-based deterrence components move from the option most common and readily deployable option (Criminal Action), to the most severe (Kinetic Action), an option of last resort.

Criminal Action

The naming of individuals by the U.S. government for breaking laws associated with cybercrime has three potential deterrent objectives: 1) to bring a criminal to justice via jail or other penalty, 2) to cause international embarrassment, e.g., "naming and shaming" or 3) to limit the travel of the named person for fear of arrest and/or extradition. A large number of early U.S. cybercrime actions were filed against Chinese companies, Chinese military and/or Chinese civilians with the primary objective of naming and shaming. More recently, Russian hackers have been identified, placed on most-wanted lists, and in some cases have been extradited and are pending prosecution

- At present, criminal action within cyberspace has produced mixed results: November 2012: Chinese attackers relentlessly attacked a small family-run business where for 3 years before agreeing to settle the lawsuit out of court. In the process, the company nearly collapsed as the hackers attacked both the business and the supporting legal team.[44]

- July 2013: U.S. prosecutors sought a 20-year prison term against a Russian attacker, claiming he caused $300 million in losses for hacking 17 retailers, financial institutions and payment processing companies. The individual was extradited from Netherlands to the U.S. in November 2014, and prosecutors achieved both imprisonment for him, and embarrassment for Russia the Russian government.[45]
- May of 2014: The U.S. levied criminal charges against five Chinese military hackers, accusing them of stealing trade secrets and other proprietary or sensitive information online. This move by the U.S. government was identified as the first defense-related prosecution. The Department of Justice named officers in the Chinese People's Liberation Army as perpetrators in the first-ever case of economic espionage charges against hackers working for a foreign government.[46]
- February 2015: FBI announces a reward of up to $3M for arrest and/or conviction of Evgeniy Mikhailovich Bogachev, for his alleged involvement in a major cyber racketeering enterprise.[47] Bogachev is also said to be the mastermind behind the CryptoLocker Ransom ware responsible for holding computer users hostage via encrypting all of their data until they pay ransoms.[48]

Although first on the list of the framework escalation, the importance of identifying individuals can limit the further physical movement of individuals and/or leaders of organizations. This may have a greater impact on individual hackers and Cyberactivists than nation state actors.

Diplomatic Demarche

Assuming there is a strong case supporting attribution, the U.S. administration may use diplomatic channels to formally protest via a diplomatic demarche to the offending foreign government in response to its actions and/or policies. The demarche may also be accompanied with economic sanction(s) including, but not limited to, trade restrictions.

Economic Response

The use of economic sanctions today is varied, and can include the adoption of policies such as trade barriers, restrictions on financial transactions or supply chain disruption. In 2010, then Secretary of State Hillary Clinton was one of the first senior USG officials to publically state the U.S. would consider the use of Economic Sanctions as a viable option during a cyberwar when

she said "…countries that knowingly permit cyberattacks to be launched from their territories would suffer damage to their reputations, and could be frozen out of the global economy."[49]

Economic sanctions have become a powerful option in the U.S. government's toolbox. In his paper, Edward Luttwak made the claim that: "the methods of commerce are displacing military methods – with disposable capital in lieu of firepower, civilian innovation in lieu of military-technical advancement, and market penetration in lieu of garrisons and bases"[50]

Whereas, a cyberattack may occur in milli- or nano-seconds, the impacts of economic sanctions are orders of magnitude slower in response. As a state traditionally considers distinction and proportionality in responding to an attack, timeliness of response creates a new consideration and nuance to response sequencing with respect to cyber.

Offensive Cyber Response

An offensive cyber response refers to U.S. capability to retaliate against an attacker with the means and methods exclusive to cyberspace. These activities may influence a physical infrastructure or result in communication disruption, such as that seen in 2007 when massively coordinated Russian cyberattacks disrupted the communications and operations of Estonia's banks, parliament, ministries, newspapers, and TV.[51] Considering that the majority of offensive cyber capabilities are highly classified, the public may not know the U.S. retaliated with an offensive cyberattack. However, it is important for the sake of deterrence would-be attackers know retaliation within cyberspace is part of the U.S. cyberattack response arsenal.

The response of an Offensive Cyber response may be on the same order as that of a cyberattack, but automated Offensive Cyber response have many risks (attribution, distinction considerations, etc.) wherein a risk averse Cyber Offensive response will likely take a minimum of hours to days to employ.

Coordinated Ally Response

Employing international support is critical if: 1) the U.S. has been incapacitated and cannot respond and, 2) the U.S. does not have the intelligence to identify the attacker, thus inhibiting its ability to respond.

Ideally, an international coalition of like-minded organizations with an established agreement to collate and leverage their cyber knowledge and attribution methodologies could greatly improve the probability of identifying a cyber attacker. It is important to note, this international coalition does not need to be made up of government entities alone. As addressed throughout this paper, unlike nuclear deterrence, cyber deterrence relies on a combination of civil society, non-government entities, and the government.

The 2014 Russian cyberattack on the White House, for example, was discovered not by the U.S., but rather an ally.[52] This highlights the importance of cooperation among allies, and the ability to garner international support for timely and coordinated responses to cyberattacks.

Kinetic Response

The rung, hopefully the least used rung, on the escalation response continuum includes the use of conventional or even nuclear weapons in response to a cyberattack. Advancing to a kinetic response must be done with thoughtful consideration, and it is critical to include in the range of options. Advancing to this last rung crosses a line, but it is a line the U.S. must be prepared to cross. In the words of the former Commander of CYBERCOM, General Alexander, "If [the cyberattack] destroys government or other networks, I think it would cross that line."[53]

In the event of an existential cyberattack or an event that drastically impairs the existence of our society, nuclear weapons should be on the table as a last resort. As the denial based deterrence is strengthened, the likelihood of a nuclear response is low and commensurate with the equally unlikelihood of an existential cyberattack. Basic services and infrastructure that sustain life in the U.S. depend on the Internet (e.g., food distribution, power, monetary system, etc.). The protection and defense of this infrastructure is essential.

Chapter 3: How Cyber Deterrence Should Be Implemented

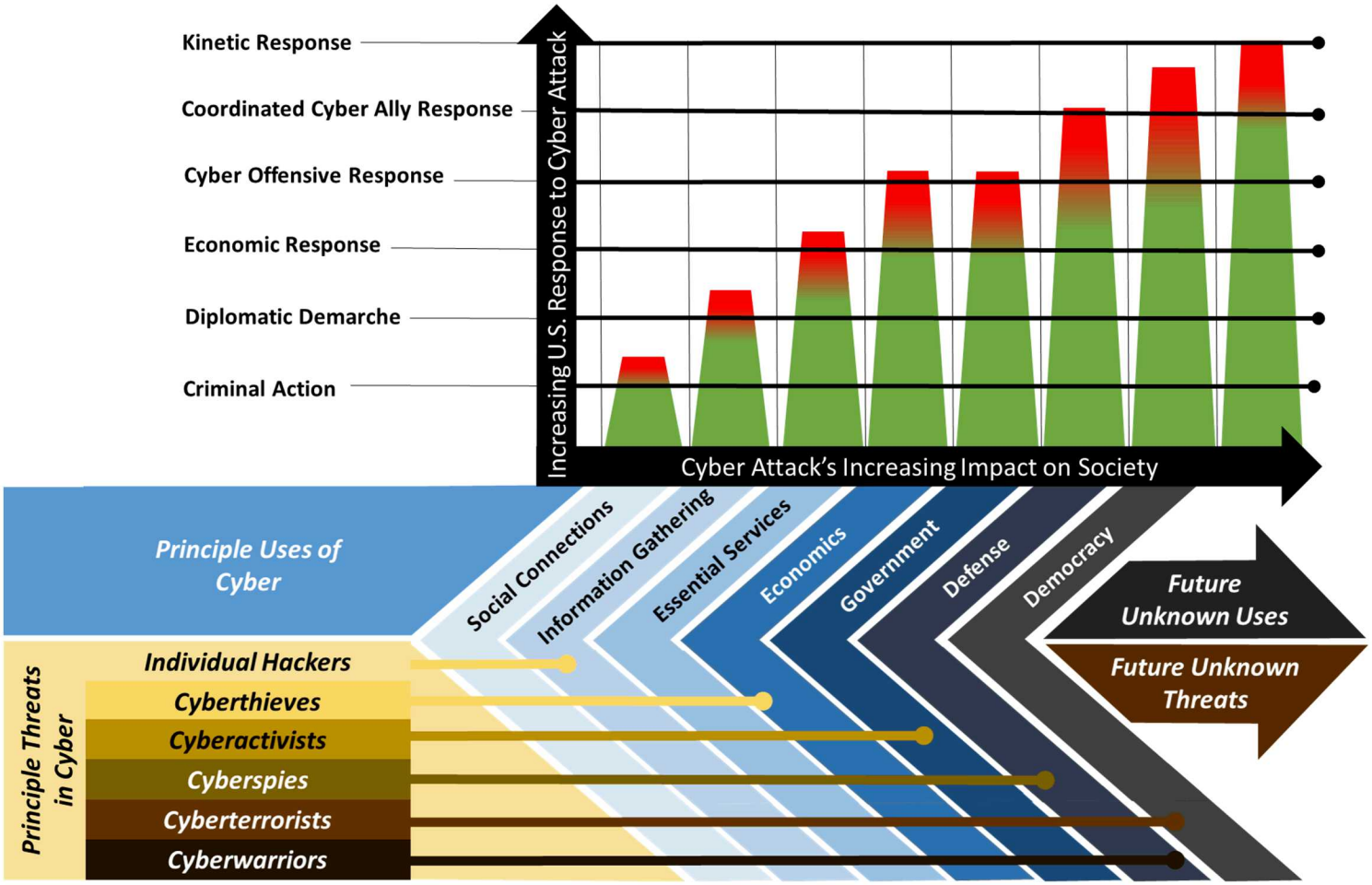
The power of the cyber deterrence escalation framework is that it communicates to would-be attackers how the United States government will respond when threatened in cyberspace.

The next step is for U.S. policy makers to determine which rung of the ladder should be used in response to a cyberattack. When considering advancing through the rungs on the ladder, especially into the use of force, key elements of the Laws of Armed Conflict should be considered, including: military necessity, proportionality of response, and the prohibition against attacking non-combatant targets.

The amount of physical damage caused by an attack is not the only factor when determining proportionality, especially when the attack occurred in or from cyberspace. From a physical damage perspective, previous cyberattacks on the U.S. may seem relatively small and inconsequential, (e.g., no loss of life and no bombs detonations). But, from an economic or even social perspective, cyberattacks can cause significant damage. Attacks launched via cyberspace can cause great damage to critical U.S. infrastructure such as energy, banking, hospitals, etc. Beyond the physical damage, confidence in the system may also be compromised and lead people to not use the system; the same result as if the system were physically destroyed.[54] Depending on the length of downtime and scope of disturbance caused by the cyberattack, the proportionality of a given response may change.

To provide a means to determine proportionality, the framework adds another axis entitled "Uses of Cyberspace," as shown in Figure 2. The intent of this axis is to help policy makers determine what is at stake as a result of a cyberattack. One end of the axis describes how individuals use cyberspace integral to present day Western society. On the other end, the axis addresses how a cyberattack could potentially impact the survival of U.S. society, as we know it.

FIGURE 2 ANALYTIC FRAMEWORK WITH "USES OF CYBERSPACE" AXIS



While the portion of the framework that contained policies and programs for cyber defense is critical, Figure 2 focuses solely on how the U.S. will respond after a cyberattack. The "Uses of Cyberspace" axis provides a guide to correlate the appropriate response to the cyberattack based on how the attack impacts U.S. national interests. This guide, as indicated by the green area, shows that criminal action will be the typical response to a cyberattack, while the use of nuclear weapons is reserved for those unknown future threats that pose an existential risk to the United States.

The following sections briefly describe the common uses of cyberspace, as stated in Figure 2.

Principle Uses of Cyberspace

Social Connections

The ability of individuals and/or groups to communicate easily with one another via cyberspace, with little to no cost, was as revolutionary as the printing press was over 500 years ago. As cyberspace evolved, individuals could now publish content themselves and share it globally. Web platforms have also facilitated the connection between individuals and groups that perhaps would not have connected outside of their shared "online" interests. The Obama Administration describes cyberspace as a platform for the free exchange of ideas.[55]

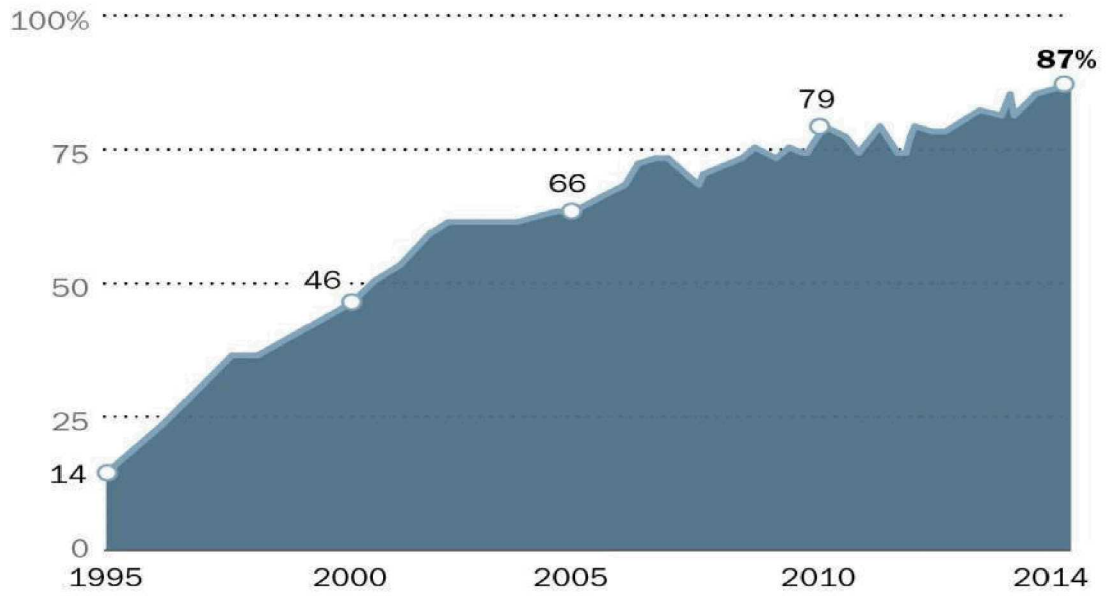
Information Gathering

People are connected and have access to more information than ever before. Organizations, both public and private, are more horizontally integrated as a result of the ease of access to information via cyber; leaders do not control the flow of information as they once did as the masses have access to the same information…in real time.

Additionally, the ability to send information real time via one or many web-based communication platforms to a specific group has changed the way in which we distribute information. Other activities rounding out the top list of informational uses of cyberspace includes: online searches, shopping, and banking/financial transactions.[56] The following chart demonstrates how pervasive the use of cyberspace is to daily life and in the U.S.

FIGURE 3 U.S. INTERNET USE, 1995-2014: PERCENT OF AMERICAN ADULTS WHO USE THE INTERNET

Source: Pew Research Center surveys, 1995-2014[57]



A May 2011 Pew Internet survey found that 92% of online adults use search engines to find information on the Web, including 59% who do so on a typical day. This places searches at the top of the list of most popular online activities among U.S. adults. But it is not alone at the top. Among online adults, 92% use email, with 61% using it on an average day.[58]

Essential Services

Essential services are systems and services that support the basic needs of society, including: financial systems, power grids, health systems, air traffic control systems, telecommunication systems, and agriculture systems.

According to The Pew Research Center, "51% of U.S. adults, or 61% of Internet users, bank online; 32% of U.S. adults or 35% of cell phone owners, bank using their mobile phones."[59]

A cyberattack against a U.S. critical infrastructure company has the potential to cause serious harm to U.S. daily life and national security. Attacks targeting Supervisory Control and Data Acquisition (SCADA) systems – the systems most often used to manage most critical infrastructure industries – could cripple these essential services, effectively crippling U.S. society. Real-world examples of this type of potentially crippling cyberattack include the attacks against Saudi Aramco and the STUXNET operation; both cases saw the large-scale destruction of

software and hardware. On U.S. soil, Sony Pictures Entertainment and the German Steel Mills [60] experienced crippling work stoppage cyberattacks. While neither the Sony nor German Steel companies are considered part of the U.S. critical infrastructure, these cyberattacks represent a troubling increase in the number of cyber espionage/cybercriminal attacks. Adversaries aggressively pursue U.S. Intellectual Property (IP), trade secrets, and other proprietary business practices that undermine U.S. businesses in the marketplace. The Sony case has the added element of political coercion; a hostile nation-state held movie theater chain hostage and threatened U.S. citizens if the movie "The Interview" was shown. If a cyberattack were to occur on U.S. soil against a critical infrastructure firm, the U.S. Government must to be in a position to react and respond – nationally and internationally – in a timely and decisive manner.

Economics

Cyberattacks related to economics apply to any attack that impacts U.S. economic growth, including digitally deliverable services.[61] In his speech during the February 2015 Cyber Summit at Stanford, President Obama said: "So much of our economic competitiveness is tied to … America's leadership in the digital economy." The Internet, he emphasized, is an engine for economic growth, further adding, "As a nation, we do more business online than ever before -- trillions of dollars a year."[62]

Societies can only flourish in safe, stable environments. Stable environments then give way to economic development.[63] Attacks and threats in cyberspace seek to disrupt stability, and thus impact our economic growth.

Economic impacts are not just attacks via cyberspace, but also via espionage. "Chinese spies are responsible for nearly $300 billion a year in stolen intellectual property, lost business to American companies, and … Americans jobs."[64]

Government

U.S. Government computer networks – specifically unclassified email – remain vulnerable to cyberattacks. The Department of State, the White House, the Office of Personnel Management and the U.S. Postal Service have all reported network intrusions to their unclassified systems. The USPS reported in 2014 that personal data for over 800,000 employees and data from customers using the call center might have been compromised.[65] In 2013, Anonymous, the

loosely affiliated group of cyberactivists, published a link with 2,000 emails and passwords, a large number coming from the House of Representatives. Also included were emails from the Office of the U.S. Attorney General and the U.S. Senate. According to Nextgov.com, 16 federal government agencies do not use a multi-layered authentication profile – e.g., password only, without key card – which make them more susceptible to malware attacks.[66]

Defense

The United States military uses cyberspace to project power globally on a "scale far greater than our adversaries."[67] The use of cyberspace to enable the defense of the U.S. ranges from the technology in the weapon systems to the technology used for command and control and a range of uses in between. However, the defense of the U.S. is not just the military, but also the businesses that support the Department of Defense. The U.S. defense industry base includes companies that develop products for the military, companies that build parts and maintain electrical systems, financial systems, etc.

Democracy

One of the first things the U.S. government does when there is a revolution taking place on the streets of a repressive society is to try and bring in Internet servers so ordinary people can communicate.[68] U.S. government policy is that more information sharing among people on the street is likely to yield more democratic institutions.[69] Cyberspace has now enabled a new form of collective activism through social media and social networking platforms.

The Arab Spring is an example of how social media was used as a tool to facilitate communications and organize protests. "Social media tools are not a replacement for real-world action but a way to coordinate it."[70] Cyberspace and social media platforms are tools used to enable the quick dissemination of information with other like-minded people and to coordinate activities.

The connectivity provided via cyber and the information that enables people is essentially a symbol of freedom. The impact of a cyberattack on freedom of individuals and society as a whole may constitute the use of kinetic weapons in response.

Principle Threats in Cyberspace

In addition to the "Principle Uses of Cyber" axis described in the Figure 2 escalation framework, a "Principle Threats in Cyber" axis was also added to correlate who typically attacks what in cyberspace. In "The Art of War", Sun Tzu states: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat." Knowing the enemy and their motivations is critical for deterrence as deterrence is essentially seeking to modify the behavior of the would-be attacker. Categorization by motivation and target in cyberspace provides a deeper understanding of motivation and aids in the determination of response proportionality for behavior deterrence. The recently published Congressional Research Service paper "Cyberwarefare and Cyberterrorism: In Brief" provides is the reference for the terms used to describe some of the key cyber threats and their motivations:[71]

Table: Key Cyber Threats

Cyber Threat	Motivation
Individual Hackers	Ego, personal enmity
Cyberthieves	Economic gain
Cyberactivists	Political and/or social action
Cyberspies	Competitive gain for strategic, financial or political advantage
Cyberterrorist	Political or social change
Cyberwarriors	Political or military gain

Individual Hackers

Computer "hackers" were some of the first to believe that "access to online information was a universal human right."[72] Oftentimes network systems were targeted and exploited via questionable technical means simply because it could be done.

Cyberthieves

"Cyberthieves are individuals who engage in illegal cyberattacks for monetary gain."[73] Cybercrime is the use of digital tools by criminal enterprises to steal and/or commit illegal acts. According to Singer and Friedman, "credentials fraud" is the most pervasive kind of cybercrime, involving "the misuse of account details to defraud financial and payment systems." Other cybercrime attacks involve exploiting advertising revenue via automated click-fraud, or by "typo-squatting" – registering a web domain with a slightly different spelling to collect ad revenue from people that visit the site in error.[74] Cybercrime deterrence in the private sector is largely the responsibility of private industry. Often, companies do not employ IT best practices and training until after a major cybersecurity incident. JP Morgan Chase & Co., the largest U.S. financial institution, plans to double its IT security budget to approximately $500 billion over 5 years after it was hit in 2014 with a major cyberattack.[75]

Cyberactivists

Cyberactivists ("hacktivism") use their cyber skills to promote political/social change by using debatable cyber means of protest, including launching malware, defacing a web page, or overwhelming a target site with "the power of the crowd" – in other words, sending so many people to a site so as to flood or hinder Internet traffic.[76] A well-known cyberactivist organization, the "shadowy international group of loosely affiliated hackers known as Anonymous,"[77] often target entities they perceive as having committed a social injustice. When several financial institutions stopped processing payments to WikiLeaks, Anonymous attacked those companies for punishing, in Anonymous' opinion, a legitimate whistle-blower on U.S. government corruption. One deterrence strategy to counter the actions of cyberactivists may simply be to wait out the attack Another strategy – although not practical in most scenarios – is for the target of a cyberattack to "hack back," but then the threat of escalation comes into play.

Cyberspies

"Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage." These individuals work at the behest of, and take direction from, foreign government entities."[78] A California-based software firm saw its business erode with the illegal theft of its proprietary

software. Additionally, once the owner publically sought recourse by publically naming China as the offender and pursued litigation, the small software firm was the victim of a non-stop cyberattack campaign that nearly bankrupted the company.[79]

Cyberterrorists

"Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives."[80] The FBI defines cyberterrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[81] Therefore, a true "terrorist" event, as defined by the FBI and other USG agencies, involves some kind of violent act against non-combatants. To date, no cyberattack has caused the loss of life, but loss of life is not unimaginable considering the number of critical service industries in the U.S. (e.g., medical, banking/finance, power, water, gas), which wholly function on web-based systems – systems that remain vulnerable to cyberattacks. It should also be noted the dual-use nature of the cyber physical world. As the Internet of Things continues to propagate, first responder and other essential life-sustaining services become prime targets of opportunity for attacks to cause life-threatening damage. Still, most, if not all of the positive Internet uses have negative ones as well. People, groups and organizations are better connected, including bad people, bad groups, and bad organizations. Deterrence efforts against terrorists looking to use cyber to carry out acts of terrorism will depend on the ability of the U.S. to track and monitor known terrorist organizations and their use of email, social media and other cyber platforms.

Cyberwarriors

"Cyberwarriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives. These entities may or may not be acting on behalf of the government with respect to target selection, timing of the attack and type(s) of cyberattack…"[82] A good example of a cyberattack perpetrated by cyberwarriors was the recent attack on U.S.-based Sony Pictures by (agents for) North Korea. Nation states are familiar with the consequences of the discovery of traditional espionage against other nation states. When a spy is discovered in a foreign country, diplomatic and criminal conventions apply. There are yet to be established boundaries, norms, and expected retaliation for cyber espionage. Many compare the atmosphere on the Internet to the "Wild West" or the early days of sea

exploration wherein the only difference between a pirate and a privateer was a government commission. Deterrence with regard to nation-sponsored cyber espionage will likely need to be addressed in an international forum.

Chapter 4: An Example of Cyber Deterrence Strategy Implementation

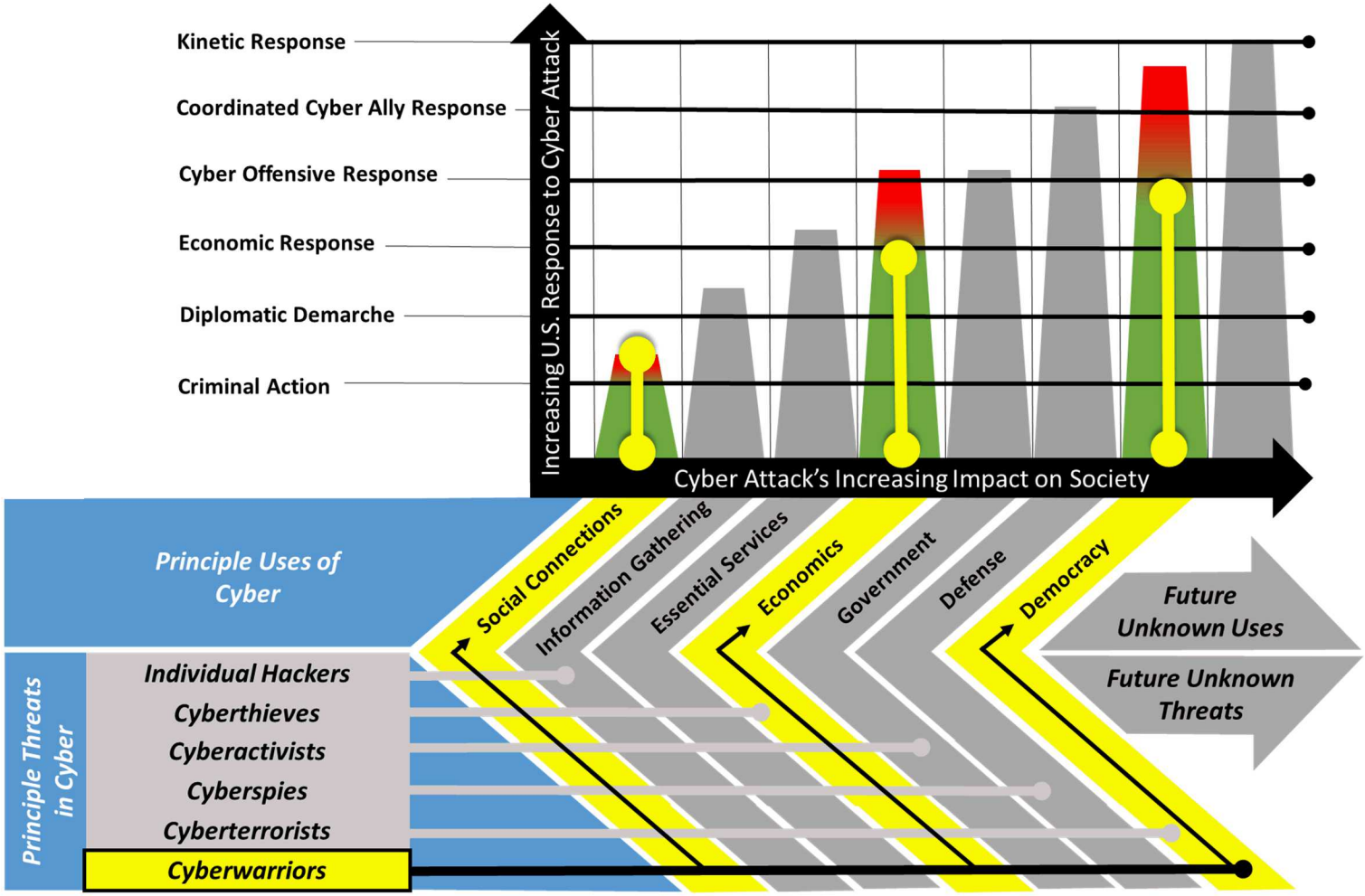
We live in a world where an attack on the movie industry receives more public attention - and visible government response - than the constant attacks on local,[83] city/state,[84] federal government,[85] or the National Defense Industry.[86] The cyberattack against Sony Pictures Entertainment in November 2014 provides an excellent case study to assess the Cyber Deterrence Analytic Framework.

The attack on Sony was triggered by the production of the movie "The Interview," a farce about an assassination plot against the Kim Jung-un, leader of the Democratic People's Republic of Korea. Cyber attackers, known as the "Guardians of Peace," initially sought to embarrass Sony, however the attack quickly elevated to threats of mass violence if the film were released in U.S. movie theaters. Additionally, the Guardians of Peace threatened to release the private information of hundreds of Sony Pictures' employees, known as "doxing," that they stole from the Sony computer network. The theft and loss of business should not be understated, but individuals and firms can survive short-term inconveniences. However there were two vital interests that were key drivers to a U.S. Government response: 1) state sponsored threats to U.S. lives and, 2) state sponsored threats to liberty and democracy by silencing freedom of speech. These two issues raised this cyberattack to a new level.

Figure 4 utilizes the Cyber Deterrence Analytic Framework by first highlighting portions of the framework applicable to how the attack impacted Sony. The attack was destructive on many levels: theft and exposure of internal corporate communications, theft of proprietary information (yet-to-be- released films and scripts) and, destruction of computer systems/hardware.

Figure 4 also highlights which type of threat category descriptive of the hackers that attacked Sony. In this case, what took the Sony Pictures Entertainment cyberattack to a new level was the threat of violence by the attackers if a particular film was released in theaters. This threat of violence to citizens across the United States gave credence to escalating the response actions.

FIGURE 4 ANALYTIC FRAMEWORK APPLICATION: SONY PICTURES



Since the attackers of Sony stole personal and industrial data, the "social" and "economics" uses of cyber are highlighted in yellow in Figure 4. Figure 4 also highlights "democracy" in yellow because this cyberattack caused a visceral reaction among the American public, as it was a direct attack on American democratic principles and way of life. The U.S. has experienced cyber-based theft of corporate data and individual national states have restricted civil liberties of their own citizens, but the idea of a communist nation state threatening the civil liberties of U.S. citizens on U.S. soil was dramatic and caused a national rise not seen from any other previous cyberattacks.[87] In addition, the Sony incident showed the incongruity between response of a private firm and the existing U.S. Government policy of not negotiating with terrorists.

The following outlines the U.S. response to the 24 November 2014 cyberattack against Sony Pictures as applied to the Cyber Deterrence Analytic Framework:

- **Pre-Emptive Cyber Efforts**
  - The U.S. inserted "early warning radar" into cyberspace that enabled the quick attribution of the Sony attack to North Korea[88]
- **Criminal Action**
  - 1 Dec 2014: FBI begins criminal investigation[89]
- **Diplomatic Demarche**
  - 19 Dec 2014: FBI states that North Korea is behind the attack and President Obama states the U.S. "will respond proportionally"[90]
  - 22 Dec 2014: DoS calls on North Korea to compensate Sony for losses caused by the attack[91]
- **Economic Sanctions**
  - 3 Jan 2015: President Obama signs an executive order imposing economic sanctions on North Korea in reaction to the cyberattack. The sanctions target North Korea's Intelligence Bureau, which is responsible for North Korea's cyber operations[92]
- **Offensive Cyber Response**
  - 23 Dec 2014: North Korea's Internet is taken down. Cause is unknown, but speculation is North Korea did not take down its own Internet. [93]
- **Request International Support**
  - 22 Dec 2014: The U.S. requests China's help in stopping North Korea's ability to send malicious code around the world.[94]

Once the key steps the U.S. took in response to the Sony Attack are culled together, it does appear the U.S. took a comprehensive, well-rounded response approach thus establishing a precedent for a U.S. Cyber Deterrence Strategy. The next critical step is to codify the U.S. Cyber Deterrence Strategy so potential adversaries know in advance how the U.S. will respond. The proposed Presidential Policy Directive in Chapter 5 is the recommended policy codifying the U.S. Cyber Deterrence Strategy.

The Sony cyberattack case study also reinforced various themes stated throughout this paper:

1. **Cyber is New Form of Warfare:** Attacks in cyber are escalating to a new form of warfare as described in Senator John McCain's response the Sony Attack: "this is a manifestation of a new form of warfare when you destroy economies, when you are able

to impose censorship…It's more than vandalism. It's a new form of warfare that we're involved in and we need to react and we need to react vigorously."[95]

2. **No Norms of Behavior in Cyber:** "There are no agreed rules of the road in terms of cyber warfare in the way there are existing broad rules of the road for other security issues -- even if they are frequently violated."[96]
3. **Deterrence Can Be Achieved in Cyber:** "In a statement, Treasury Secretary Jacob J. Lew suggested that the sanctions were intended not only to punish North Korea for the hacking of Sony — which resulted in the destruction of about three-quarters of the computers and servers at the studio's main operations — but also to warn the country not to try anything like it again."[97]

What the Sony Hack also identified is the potential for quick escalation in cyberspace. For instance, the original attack on November 24, 2014, was motivated because another country was upset with content in something as simple as a movie. Less than a month later, tensions had escalated such that on 27 Dec 2015 the Guardians of Peace threatened to attack "the White House, the Pentagon and the whole U.S. mainland."[98] The escalation of cyberattacks, both within and without cyberspace, is an area that requires further exploration in additional studies.

Chapter 5: Proposed U.S. Cyber Deterrence Strategy Implementation Memo

The Obama Administration is currently pursuing five key priorities in cyberspace that "will strengthen our approach to cybersecurity threats."[99] They are:

1. Protecting the country's critical infrastructure from cyber threats.
2. Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.
3. Engaging with international partners to promote Internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.
4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.
5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.[100]

Recommend a sixth priority:

6. Advancing our cyber response policies and capabilities to further protect the country's national interests by deterring attacks within cyberspace.

This priority should be supported by establishing a National Cyber Deterrence Strategy, to include the adoption of the Cyber Deterrence Analytic Framework and the implementation of the following draft Presidential Policy Directive:

The White House

March XX, 2015

Recommended Draft Presidential Policy Directive -- United States Cyber Deterrence Policy

PRESIDENTIAL POLICY DIRECTIVE/PPD-XX

SUBJECT: United States Cyber Deterrence Policy

The Presidential Policy Directive on United States Cyber Deterrence communicates to the national and international communities that the United States considers cyberattacks on U.S. national interests a form of warfare and will result in a U.S. response to defend threatened national interests.

Introduction

Society's use of cyberspace continues to evolve since its beginnings as a defense and academic research project in 1960. The cyberspace domain is now an intimate part of American, and global, life. In the United States, reliance on this new domain ranges from cyber's ability to connect individuals and groups globally; to its ability to enable our electrical, transportation and health systems; to its importance in building our economic strength; to its decisive role in supporting and enabling armed conflict.

Capitalizing on society's increased reliance on cyber space, there are conversely many nefarious uses of cyber by individual, state and non-state actors who wish to exploit and harm U.S. national interests. Protection of U.S. citizens, businesses and critical infrastructure are vital to the nation as outlined in the Presidential Policy Directive (PPD) 21. When cyberattacks occur, they have significant implications for U.S. national security and foreign policy interests. Therefore, it is critical that the U.S. has a comprehensive policy for responding to cyberattacks.

The U.S. recognizes the symbiotic relationship that exists between commercial critical infrastructure owners and the U.S. government. The policy on Critical Infrastructure and Resilience (PPD-21) advances the nation's effort to strengthen and maintain the security of critical infrastructure, including cyberspace. However, defense against cyberattacks is not achievable via resiliency alone. The complement of a strong deterrence policy is also necessary

to achieve a comprehensive approach for the protection U.S. citizens, businesses, and government in cyberspace.

This directive establishes a United States cyber deterrence policy, which defines the U.S. response to significant cyberattacks against national interests. This cyber deterrence policy permits the response to a cyberattack in an escalatory manner that not only responds to the threat, but also seeks to neutralize and/or deter the initial attack from taking place.

Policy: U.S. Cyber Deterrence

The policy of the United States is to utilize all appropriate instruments of power to respond to any cyberattack that impacts the nation's interests. PPD-20 established processes and principles to integrate cyber tools into the full array of national security tools. Attacks that occur in cyber space have the potential to reverberate outside cyberspace. Therefore, the U.S. will not be constrained to limit its response to the cyber domain alone.

The Federal Government shall implement this directive in a manner consistent with applicable law, Presidential Directives, Federal Regulations, International norms and laws of warfare.

Goals of U.S. Cyber Deterrence Policy

United States cyber deterrence policy serves the following U.S. national security and foreign policy goals:

1. Promote critical infrastructure protection, and other homeland security priorities.

2. Ensure U.S. military forces, and those of allies and partners, continue to enjoy technological superiority over potential adversaries.

3. Combat transnational organized crime and related threats to national security, including the theft of intellectual property and its adverse effects against the U.S. economy and loss of competitive advantage by U.S. companies.

4. Ensure cyberattacks do not contribute to human rights violations or violations of international humanitarian law.

5. Prevent the proliferation of cyberattacks and cyber weapons.

6. Enhance the ability of allies and partners to deter or defend themselves against aggression.

7. Support democratic governance and other related U.S. foreign policy objectives.

8. Encourage the maintenance and expansion of U.S. security partnerships with those who share our interests, and regional access in areas critical to U.S. interests.

9. Promote regional stability, peaceful conflict resolution, and arms control.

Principles Governing the Cyber Deterrence Policy

The U.S. cyber deterrence policy utilizes an analytic framework, which includes two main components: denial-based deterrence and punishment-based deterrence. The denial-based deterrence is outlined in PPD-21, which was established in 2013 to strengthen the security and resilience of the United States' critical infrastructure against both physical and cyber threats.

PPD-XX comprises the punishment-based component and authorizes appropriate agencies to respond, as directed by the President, to cyberattacks on the United States' national interests.

Punishment-based deterrence will be authorized and conducted consistent with the following principles:

1. Privacy and civil liberties will be integral considerations in the planning of U.S. national cyber response activities.
2. National cyber response activities will be as tailored as feasible. In determining how to escalate the national cyber response, the United States shall consider the reliability of the attribution, resulting damage caused by the attack, and unintended international consequences of the U.S.' response.
3. When determining the appropriate national cyber response, the U.S. will choose a near-proportional response to the damage inflicted by the initial attack.

Process and Criteria Guiding U.S. Cyber Deterrence Actions

Denial-based deterrence forms the foundation of the analytic framework and includes the following activities:

- Enhancement of cyber defenses to include activities by the Department of Homeland Defense, Department of Defense, and Sector-Specific Agencies.
- Enhancement of cyber resiliency (ref PPD-21).
- Enhancement of cyber intelligence capabilities and actions as performed by the Intelligence Community and supported by the Department of Justice.
- Broadening of the federal government's involvement in cyber security by expanding cyber defensive support to critical infrastructure entities.
- Securing of supply chain procurements to ensure source companies comply with cyber security mandates.
- Robust training and quantity of cyber forces as assigned to the Departments of Defense, Homeland Security, Justice, and the Intelligence Community.
- Employment of pre-emptive measures to deny cyberattacks as indicated by intelligence of nation state or terrorist organizations supporting, or harboring, cyber attackers or cyber attacking capabilities within their borders.

Punishment-based deterrence forms the response component of the analytic framework and includes the following options the United States may use in response to a cyberattack:

- **Criminal Action**: Utilize the U.S. legal system for civil prosecution of identified cyber attackers.
- **Diplomatic Demarche**: In cases of international cyberattacks, the U.S. Government will demarche the offending government to protest a host government's policies or actions.
- **Economic Sanctions:** Includes, but not limited to: trade embargoes; restrictions on exports or imports; and denial of foreign assistance to foreign countries found to harbor, condone, or support cyberattacks or the development cyber weapons.
- **Offensive Cyber Response:** Retaliation against the attacker or attacking country with means and methods exclusive to cyberspace.
- **International Support**: If the U.S. is in a scenario where it has 1) been incapacitated and cannot respond, 2) does not have the intelligence to identify the attacker thus inhibiting the ability to respond, or 3) finds the response from another country to have greater

diplomatic implications, then the U.S. will request assistance from its allies to respond to or support response actions which could exist within cyber or take the form of a more conventional response.

- **Kinetic Response**: The escalation response continuum of a U.S. response to a cyberattack includes include the use of conventional or even nuclear weapons. While advancing to these options will not be done without thoughtful consideration, it is necessary that they are included in the range of options.

This Directive builds on guidance provided in Presidential Policy Directive/PPD-21, dated February 12, 2013.

Summary and Recommendations

On February 26, 2015, Director of National Intelligence James R. Clapper delivered the annual Worldwide Threat Assessment to the Senate Armed Services Committee. The threat assessment acknowledged cyber as a global threat and further reinforced the need for a U.S. Cyber Deterrence Strategy:

> "We foresee an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security…The muted response to cyberattacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation."[101]

Given this environment and current threats, the U.S. needs both a clear policy directive to establish a cyber deterrence strategy **and** an analytical framework to better understand how all government departments and agencies will respond to an attack. The U.S. Government should adopt a Cyber Deterrence Strategy to counter, as DNI Clapper articulated, increasing threats to our national security. Three clear and actionable steps toward a national cyber deterrence strategy include:

- Add cyber deterrence to President Obama's cyberspace priorities to specifically address deterrence against cyberattacks.
- Adopt the Cyber Deterrence Analytic Framework to assist policy makers and responsible departments and agencies in responding to cyberattacks.
- Implement the draft Presidential Policy Directive on cyber deterrence to articulate and clarify the goals, principles, and process of the policy across the U.S. Government in the event of a cyberattack.

With the U.S. Government demonstrating capability and credibility to respond to recent cyberattacks (e.g., Sony Pictures attacks), clearly articulating a policy is the final step to establishing cyber deterrence. The goal of deterrence is the modification of an adversary's

behavior: an adversary should know in advance an attack is unacceptable; with a strong cyber deterrence strategy, the enemy will know that the U.S. will respond to a cyberattack using all instruments of national power to protect U.S. interests.

Appendix: Proposed Cyber Deterrence Strategy Options Memo

To: President Barack Obama
Re: Strategic Options for Defending Against Cyber Attacks on U.S. Interests

Issue: The United States is facing a relentless threat of cyberattacks. These attacks against the U.S. government, businesses and critical infrastructure industries undermine U.S. stability and national security.

Relevant National Interests:

Vital

- Establish productive relations, consistent with national interests, with nations that could become our strategic adversaries, China and Russia.
- Ensure the visibility and stability of major global systems (communications, trade, financial markets, supplies of energy and the environment)

Extremely Important

- Maintain a lead in key military-related and strategic technologies, particularly information systems
- Suppress transnational crime.

Important

- Maintain an edge in the international distribution of information to ensure that American values continue to positively influence the cultures of other nations.[102]

Analysis/Background:

With the **number** of attacks increasing, the **threats** to the U.S. national security increasing, and the **American public more concerned** with cyberattacks, it would seem logical the U.S. Government would take concrete steps to thwart cyber threats to national security. Concrete steps, however, are not easy to take when it comes to cyberspace. The Congressional Research Service recently reported, "…no major cybersecurity legislation has been enacted since 2002."[103]

Moreover, NATO resumed its discussions on cyber, but kept the focus on defense and alliance support with more talks to follow.[104] The U.S. government must take a leadership role in cybersecurity to protect our interests and that of our allies.

Operational Objectives:

- Shape the world order in defining cyberattacks and cyberwarfare.
- Demonstrate confident leadership and defined actionable response to prevent the degradation of confidence and capability in our information systems.

Strategic Options:

Option 1: Current Strategy - "*Classified Proportionality"*

Current U.S. policy power towards cyberattacks remains highly classified and off limits to the U.S. people and most of industry. In his response to the Sony attacks, President Obama said, "We will respond. We'll respond proportionally, and we'll respond in a place and time and manner that we choose."[105] Decisions and information control/dissemination are placed solely in control of the U.S. Government.

Pros:

- U.S. leadership demonstrated it was engaged and firm in the face of the attack
- Allowed flexibility in action/domain and proportionality
- Allowed response to be conducted without media/public scrutiny

Cons:

- Lack of transparency, consistency in the face of adversary attacks and public scrutiny
- Public/industry will take matters into their own hands if proportionality is not visible.
- Dissuasion via deterrence must be clear, credible and actionable. This does not satisfy all of the conditions and risks losing credibility if attacker does not know they are being punished.
- Allows media increased power to interpret response and guide the message to the public based on lack of void (example: New York Times reporting guided by Snowden release)[106]

Option 2: *"Deterrence Strategy"*

The U.S. Government must have a cyber deterrence strategy that is easily communicated to both the national and international communities. The proposed deterrence framework emphasizes: 1)

communicating the strategy across the USG and key industry stakeholders, 2) framing options for response to a cyberattack with escalation options and, 3) deterring the adversary by demonstrating leveraging denial and demonstrating punishment based responses.

Pros:

- Acknowledges the US leadership in responding to conflict and provides a basis for NATO engagement.
- Answers the call from industry/public to respond in the face of attack.
- Leverages the step forward in diplomatic relations created by U.S.-China climate agreement.

Cons:

- US will be forced to respond in the face of attack.
- Proportionality+1 may be scrutinized and perceived as nation state dominance

Option 3: *"Focused Denial"*

The central premise of this option is for the U.S. to lead the world and focus attack defense on the development and implementation of system wide denial based punishment systems. This would include, but not be limited to: enhanced network defense, resiliency, supply chain security, improving cyber intelligence sources, larger and increasingly robust efforts to develop cyber forces and pre-emptive cyber efforts.

Pros:

- Takes advantage of U.S. strengths in technology development
- Development of additional US jobs
- Preserves US influence/cooperation in the region while assuring our allies

Cons:

- Requires substantial increases in military/intelligence budgets as well as budgeting for nationwide operations and sustainment in the face of fiscal austerity
- Controlling interest in the development and fabrication of cyber products are currently not under control of the U.S. government. Industry would require strong reasons (legislative/incentives, etc.) to participate
- May required reduction in civil liberties for public systems to have full protection

Recommendation: ***Option 2*** - *"Deterrence"*

Implementation:

Leverage the roll out of published US norms for cyber, working in parallel with this policy of deterrence. Leverage denial based deterrence opportunities outlined in PPD-21. These two activities combined with an update on the formation of the National Cyber Threat Intelligence Integration Center (CTIIC) provide a trifecta of action towards the reduction of cyber threats.

End Notes

Executive Summary

[1] Dean Williams, *Leadership for a Fractured World : How to Cross Boundaries, Build Bridges, and Lead Change*, First edition. (San Francisco: Berrett-Koehler Publishers, 2015), 35.

[2] "Department of Defense Cyber Strategy 2015" (Department of Defense, April 17, 2015). <http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

Chapter 1

[3] Nicole Perlroth, "Hacked vs. Hackers: Game On," *Bits Blog*, December 2, 2014. <http://bits.blogs.nytimes.com/2014/12/02/hacked-vs-hackers-game-on/>.

[4] T. V. Paul, Patrick M. Morgan, and James J. Wirtz, *Complex Deterrence : Strategy in the Global Age* (Chicago: University of Chicago Press, 2009), 345.

[5] "U.S. Defense Chief Warns of Digital 9/11," October 11, 2012. <http://blogs.wsj.com/cio/2012/10/11/u-s-defense-chief-warns-of-digital-911/>.

[6] CBS/AP, "Sony Pictures Hackers Make Threat over 'The Interview,' Reference 9/11," accessed December 19, 2014. <http://www.cbsnews.com/news/sony-pictures-hackers-make-911-like-threat-over-the-interview-release/>.

[7] Perlroth, "Hacked vs. Hackers."

[8] ---.

[9] Bruce Stokes, "Extremists, Cyber-Attacks Top Americans' Security Threat List," *Pew Research Center*, accessed February 26, 2015. < http://www.pewresearch.org/fact-tank/2014/01/02/americans-see-extremists-cyber-attacks-as-major-threats-to-the-u-s/>.

[10] Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions* (Congressional Research Service, June 20, 2013), 2. < http://fas.org/sgp/crs/natsec/R42114.pdf>.

[11] Sydney Freedberg, "NATO Hews To Strategic Ambiguity On Cyber Deterrence," *Breaking Defense*, November 7, 2014. <http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/>.

[12] Professor Joseph S. Nye, Personal Interview, December 1, 2014.

[13] David Sanger, Personal Interview, November 4, 2014.

[14] General (ret) James Cartwright, Personal Interview, September 29, 2014.

[15] Professor Graham T. Allison, Jr., Personal Interview, November 4, 2014.

[16] Colin Clark, "CyberCom Chief Alexander Lays Down Cyber Red Line; Destroy A Network, Risk War," *Breaking Defense*, February 27, 2014. <http://breakingdefense.com/2014/02/cybercom-chief-alexander-lays-down-cyber-red-line-destroy-a-network-risk-war/>; Paul, Morgan, and Wirtz, *Complex Deterrence*, 290.

[17] David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *The New York Times*, January 18, 2015. < http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html>.

[18] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security*, 1st ed. (Washington, DC: Potomac Books, 2009), 318.

[19] Ken Dilanian, "Cyber Threats Expanding, New US Intelligence Assessment Says - The Boston Globe," *BostonGlobe.com*, February 27, 2015. < http://abcnews.go.com/Politics/wireStory/cyber-threats-expanding-us-intelligence-assessment-29242332>.

[20] Clark, "CyberCom Chief Alexander Lays Down Cyber Red Line; Destroy A Network, Risk War." < http://breakingdefense.com/2014/02/cybercom-chief-alexander-lays-down-cyber-red-line-destroy-a-network-risk-war/>.

[21] Graham T. Allison, *Nuclear Terrorism : The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004).

Chapter 2

[22] Kramer, Starr, and Wentz, *Cyberpower and National Security*, 326.
[23] Thomas C. Schelling, *Arms and Influence* (New Haven, Yale University Press, 1966), 20.
[24] Allison, Jr., Personal Interview.
[25] Nye, Personal Interview.
[26] Ellen Nakashima, "NSA Allies with Internet Carriers to Thwart Cyber Attacks against Defense Firms," *The Washington Post*, June 7, 2011. < http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_story.html>.
[27] Cecilia Kang, "Sony Pictures Hack Cost the Movie Studio at Least $15 Million," *The Washington Post*, February 4, 2015. < http://www.washingtonpost.com/news/business/wp/2015/02/04/sony-pictures-hack-cost-the-movie-studio-at-least-15-million/>.
[28] "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," *The White House*, accessed November 1, 2014. < https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
[29] ---.
[30] Richard P. Quinn, "The FBI's Role in Cyber Security" (Statement Before the House Homeland Security Committee, Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies, Washington, D.C., April 16, 2014). < http://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security>.
[31] Devin Nunes, "H.R.1560 - 114th Congress (2015-2016): Protecting Cyber Networks Act," legislation, (April 27, 2015). < https://www.congress.gov/bill/114th-congress/house-bill/1560?q={%22search%22%3A[%22Cyber+Intelligence+Sharing+and+Protection+Act%22]}>.
[32] "FACT SHEET: Cyber Threat Intelligence Integration Center," *The White House*, February 25, 2015. <https://www.whitehouse.gov/node/323591>.
[33] Ponemon Institute Research Report, *2013 Cost of Cyber Crime Study* (HP Enterprise Security, October 2013. <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf>.
[34] "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)" (Department of Defense, November 5, 2012), DoD Instruction 5200.44. < http://dtic.mil/whs/directives/corres/pdf/520044p.pdf>; David Perera, "DoD Enacts Rule on Excluding Contractors Based on Supply Chain Risk," *FierceGovernmentIT*, accessed March 6, 2015. < http://www.fiercegovernmentit.com/story/dod-enacts-rule-excluding-contractors-based-supply-chain-risk/2013-11-21>.
[35] Defense Acquisition University, "Defense Acquisition Guidebook, Sec 13.2," December 3, 2014. <https://acc.dau.mil/docs/dag_pdf/dag_ch13.pdf>.
[36] Steve Zind, "GlobalFoundries Purchase Of IBM Essex Prompts Security Review," November 2, 2014. <http://digital.vpr.net/post/globalfoundries-purchase-ibm-essex-prompts-security-review>.
[37] ---.
[38] Cheryl Pellerin, "Rogers: Cybercom Defending Networks, Nation," *Defense.gov News*, August 18, 2014. <http://www.defense.gov/news/newsarticle.aspx?id=122949>.
[39] Julian Hattem, "US, UK to start cyber war games," Text, *TheHill*, (January 16, 2015. <http://thehill.com/policy/cybersecurity/229779-us-uk-to-flex-joint-cyber-muscle>.
[40] Quinn, "The FBI's Role in Cyber Security."
[41] Schelling, *Arms and Influence*, 2.
[42] ---.
[43] Paul, Morgan, and Wirtz, *Complex Deterrence*, 45.
[44] Michael Riley, "China Mafia-Style Hack Attack Drives California Firm to Brink," *Bloomberg*, November 27, 2012. <http://www.bloomberg.com/news/2012-11-27/china-mafia-style-hack-attack-drives-california-firm-to-brink.html>.
[45] Fred Pals and David Voreacos, "Accused Russian Hacker May Be in U.S. Hands Soon," *Bloomberg*, November 4, 2014. <http://www.bloomberg.com/news/2014-11-04/dutch-to-hand-russian-hacking-suspect-drinkman-to-u-s-.html>.
[46] Ellen Nakashima and William Wan, "U.S. Announces First Charges against Foreign Country in Connection with Cyberspying," *The Washington Post*, May 19, 2014. <http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html>.

[47] Federal Bureau of Investigations, "$3 Million Reward Offered for International Cyber Criminal," FBI News Blog, *FBI*, (February 24, 2015. <http://www.fbi.gov/news/news_blog/3-million-reward-offered-for-international-cyber-criminal>.
[48] ---.
[49] David E. Sanger, Thom Shanker, and John Markoff, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times*, January 26, 2010, sec. World. <http://www.nytimes.com/2010/01/26/world/26cyber.html>.
[50] Edward N. Luttwak, "From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce," *The National Interest*, no. 20 (July 1, 1990): 17–23.
[51] Scheherazade Rehman, "Estonia's Lessons in Cyberwarfare," *US News & World Report*, January 14, 2013. <http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare>.
[52] Ellen Nakashima, "Hackers Breach Some White House Computers," *The Washington Post*, October 28, 2014. <http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html>.
[53] Clark, "CyberCom Chief Alexander Lays Down Cyber Red Line; Destroy A Network, Risk War."

Chapter 3
[54] Cartwright, Personal Interview.
[55] Barack H. Obama, "Foreign Policy Cyber Security," *The White House*, accessed February 28, 2015. <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity>.
[56] "Top 10 Uses of Internet," *Before It's News | Alternative News | UFO | Beyond Science | True News| Prophecy News | People Powered News*, June 22, 2013. <http://beforeitsnews.com/alternative/2013/06/top-10-uses-of-internet-2690290.html>.
[57] Susannah Fox and Lee Rainie, "The Web at 25 in the U.S.," *Pew Research Center's Internet & American Life Project*, accessed May 12, 2015. <http://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s/>.
[58] Kristen Purcell, *Search and Email Still Top the List of Most Popular Online Activities*, Pew Internet & American Life Project (Pew Research Center, August 9, 2011. <http://www.utexas.edu/courses/kincaid/DigitalMedia/readings/130129Wk03-Email/111111PIP_Search-and-Email.pdf>.
[59] Susannah Fox, "51% of U.S. Adults Bank Online," *Pew Research Center's Internet & American Life Project*, accessed May 12, 2015. <http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/>.
[60] "Hack Causes 'Damage' at Steel Works," *BBC News*, December 22, 2014. <http://www.bbc.com/news/technology-30575104>.
[61] Jessica Nicholson and Ryan Noonan, "Measuring Bytes across Borders | Economics and Statistics Administration," January 27, 2014. <http://www.esa.doc.gov/Blog/2014/01/27/measuring-bytes-across-borders>.
[62] Barack H. Obama, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," *The White House*, accessed February 28, 2015. <http://www.whitehouse.gov/node/322201>.
[63] Derek S. Reveron, *Exporting Security : International Engagement, Security Cooperation, and the Changing Face of the U.S. Military* (Washington, DC: Georgetown University Press, 2010), 48.
[64] Shane Harris, "Exclusive: Inside the FBI's Fight Against Chinese Cyber-Espionage," *Foreign Policy*, May 27, 2014. <http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/>.
[65] Reuters, "U.S. State Department Email System Reportedly Hacked," *The Huffington Post*, November 17, 2014.
[66] Aliya Sternstein, "Fallout from Clinton's Private Emails: How Secure Are Agency Email Systems?," *Nextgov.com*, March 5, 2015. <http://www.huffingtonpost.com/2014/11/17/state-department-email-hacked_n_6170640.html>.
[67] Air Force CIO, "Air Force Cyberspace Operations Strategy 2014," 2014.
[68] Sanger, Personal Interview.
[69] *ANSX | WIKI Segment 2 | BEFORE WIKI*, 2013. <https://www.youtube.com/watch?v=kJpTjoZa2Ic&feature=youtube_gdata_player>.
[70] Clay Shirky, "The Political Power of Social Media," *Foreign Affairs*, no. January/February 2011 (February 2011). <http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media>.
[71] Catherine A. Theohary and John W. Rollins, "Cyberwarfare and Cyberterrorism: In Brief," *Congressional Research Service*, no. R43955 (March 27, 2015): 12. <http://fas.org/sgp/crs/natsec/R43955.pdf>.
[72] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014), 74.

[73] Theohary and Rollins, "Cyberwarfare and Cyberterrorism: In Brief."
[74] Singer and Friedman, *Cybersecurity and Cyberwar*, 85, 86.
[75] Hugh Son, "Dimon Sees Cyber-Security Spending Doubling After Hack," *Bloomberg.com*, October 10, 2014. <http://www.bloomberg.com/news/articles/2014-10-10/dimon-sees-jpmorgan-doubling-250-million-cyber-security-budget>.
[76] Singer and Friedman, *Cybersecurity and Cyberwar*, 77, 78.
[77] Nicole Perlroth, "Anonymous Hackers' Efforts to Identify Ferguson Police Officer Create Turmoil," *The New York Times*, August 14, 2014. <http://www.nytimes.com/2014/08/15/us/ferguson-case-roils-collective-called-anonymous.html>.
[78] Theohary and Rollins, "Cyberwarfare and Cyberterrorism: In Brief," 2.
[79] Riley, "China Mafia-Style Hack Attack Drives California Firm to Brink." <http://www.bloomberg.com/news/2012-11-27/china-mafia-style-hack-attack-drives-california-firm-to-brink.html>.
[80] Theohary and Rollins, "Cyberwarfare and Cyberterrorism: In Brief," 2.
[81] Singer and Friedman, *Cybersecurity and Cyberwar*, 96.
[82] Theohary and Rollins, "Cyberwarfare and Cyberterrorism: In Brief," 3.

Chapter 4
[83] Chris Gadd, "Dickson Sheriff's Office Pays Ransom to Cyber Criminals," *The Tennessean*, November 14, 2014. <http://www.tennessean.com/story/news/local/dickson/2014/11/11/dickson-sheriffs-office-pays-ransom-cyber-criminals/18868325/>.
[84] Holly Fournier, "Duggan: Detroit Database Held for Ransom," November 17, 2014. <http://www.detroitnews.com/story/news/politics/michigan/2014/11/17/north-american-international-cyber-summit/19162001/>.
[85] Frank Konkel, "Every Part of the US Government Has Probably Already Been Hacked," *Defense One*, September 10, 2014. <http://www.defenseone.com/technology/2014/09/every-part-us-government-has-probably-already-been-hacked/93761/>.
[86] Andy Greenberg, "For Pentagon Contractors, Cyberspying Escalates," *Forbes*, accessed January 5, 2015. <http://www.forbes.com/2010/02/17/pentagon-northrop-raytheon-technology-security-cyberspying.html>.
[87] David Weldon, "Thwarting a New Breed of Cyberattack," *FierceCIO*, January 27, 2015. <http://www.fiercecio.com/story/thwarting-new-breed-cyberattack/2015-01-27>.
[88] Sanger and Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say." <http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html>.
[89] David Robb, "Sony Hack: A Timeline," *Deadline*, December 22, 2014. <http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/>.
[90] ---.
[91] ---.
[92] Jim Acosta and Kevin Liptak, "U.S. Slaps New Sanctions on North Korea after Sony Hack - CNNPolitics.com," *CNN*, January 3, 2015. <http://www.cnn.com/2015/01/02/politics/new-sanctions-for-north-korea-after-sony-hack/index.html>.
[93] Mike Chinoy, "A Cyber Conflict with North Korea Is 'Dangerous Uncharted Territory' - CNN.com," accessed March 7, 2015. <http://www.cnn.com/2014/12/23/world/asia/north-korea-cyber-conflict-chinoy-qa/index.html>; Nicole Perlroth and David E. Sanger, "North Korea Loses Its Link to the Internet," *The New York Times*, December 22, 2014. <http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html>.
[94] ---.
[95] Jethro Mullen, "North Korea and the Sony Hack: The War of Words Escalates - CNN.com," accessed March 7, 2015. <http://www.cnn.com/2014/12/22/world/asia/north-korea-us-sony-hack-who-says-what/index.html>.
[96] Chinoy, "A Cyber Conflict with North Korea Is 'Dangerous Uncharted Territory' - CNN.com."
[97] David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony Case," *The New York Times*, January 2, 2015. <http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html>.
[98] Robb, "Sony Hack."

Chapter 5
[99] Obama, "Foreign Policy Cyber Security." <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity>.
[100] ---.

Summary and Recommendations
[101] James R. Clapper, "DNI Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community to the Senate Armed Services Committee" (DNI, February 26, 2015), 1, 2. <http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf>.

Appendix
[102] Graham T. Allison and Robert Blackwill, *America's National Interest* (Belfer Center for Science and International Affairs, John F. Kennedy School of Government, 1998. <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=189698>.
[103] Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions.*
[104] Freedberg, "NATO Hews To Strategic Ambiguity On Cyber Deterrence."
[105] Steve Holl and Matt Spetalnick, "Obama Vows U.S. Response to North Korea over Sony Cyber Attack," *Reuters*, December 19, 2014. <http://www.reuters.com/article/2014/12/19/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141219>.
[106] Sanger and Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say."

Bibliography

Acosta, Jim, and Kevin Liptak. "U.S. Slaps New Sanctions on North Korea after Sony Hack - CNNPolitics.com." *CNN*, January 3, 2015.

Air Force CIO. "Air Force Cyberspace Operations Strategy 2014," 2014.

Allison, Graham T. *Nuclear Terrorism : The Ultimate Preventable Catastrophe*. 1st ed. New York: Times Books/Henry Holt, 2004.

Allison, Graham T., and Robert Blackwill. *America's National Interest*. Belfer Center for Science and International Affairs, John F. Kennedy School of Government, 1998.

Allison, Jr., Professor Graham T. Personal Interview, November 4, 2014.

ANSX | WIKI Segment 2 | BEFORE WIKI, 2013.

Cartwright, General James (ret). Personal Interview, September 29, 2014.

CBS/AP. "Sony Pictures Hackers Make Threat over 'The Interview,' Reference 9/11."

Chinoy, Mike. "A Cyber Conflict with North Korea Is 'Dangerous Uncharted Territory' - CNN.com." Accessed March 7, 2015.

Clapper, James R. "DNI Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community to the Senate Armed Services Committee." DNI, February 26, 2015.

Clark, Colin. "CyberCom Chief Alexander Lays Down Cyber Red Line; Destroy A Network, Risk War." *Breaking Defense*, February 27, 2014.

Danzig, Richard J. "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies." *Center for a New American Security,* July 2014.

Defense Acquisition University. "Defense Acquisition Guidebook, Sec 13.2," December 3, 2014.

"Department of Defense Cyber Strategy 2015." Department of Defense, April 17, 2015.

Defense Science Board. "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat." *Department of Defense,* January 2013.

Dilanian, Ken. "Cyber Threats Expanding, New US Intelligence Assessment Says - The Boston Globe." *BostonGlobe.com*, February 27, 2015.

"FACT SHEET: Cyber Threat Intelligence Integration Center." *The White House*, February 25, 2015.

Federal Bureau of Investigations. "$3 Million Reward Offered for International Cyber Criminal." FBI News Blog. *FBI*, February 24, 2015.

Fischer, Eric A. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*. Congressional Research Service, June 20, 2013.

Fournier, Holly. "Duggan: Detroit Database Held for Ransom," November 17, 2014.

Fox, Susannah. "51% of U.S. Adults Bank Online." *Pew Research Center's Internet & American Life Project*.

Fox, Susannah, and Lee Rainie. "The Web at 25 in the U.S." *Pew Research Center's Internet & American Life Project*.

Freedberg, Sydney. "NATO Hews To Strategic Ambiguity On Cyber Deterrence." *Breaking Defense*, November 7, 2014.

Gadd, Chris. “Dickson Sheriff’s Office Pays Ransom to Cyber Criminals.” *The Tennessean*, November 14, 2014.
Greenberg, Andy. “For Pentagon Contractors, Cyberspying Escalates.” *Forbes*. Accessed January 5, 2015
“Hack Causes ‘Damage’ at Steel Works.” *BBC News*, December 22, 2014.
Harris, Shane. “Exclusive: Inside the FBI’s Fight Against Chinese Cyber-Espionage.” *Foreign Policy*, May 27, 2014.
Hattem, Julian. “US, UK to start cyber war games.” Text. *TheHill*, January 16, 2015.
Holl, Steve, and Matt Spetalnick. “Obama Vows U.S. Response to North Korea over Sony Cyber Attack.” *Reuters*. December 19, 2014.
Jethro Mullen. “North Korea and the Sony Hack: The War of Words Escalates - CNN.com.” Accessed March 7, 2015.
Kang, Cecilia. “Sony Pictures Hack Cost the Movie Studio at Least $15 Million.” *The Washington Post*, February 4, 2015.
Konkel, Frank. “Every Part of the US Government Has Probably Already Been Hacked.” *Defense One*, September 10, 2014.
Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. 1st ed. Washington, DC: Potomac Books, 2009.
Luttwak, Edward N. “From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce.” *The National Interest*, no. 20 (July 1, 1990): 17–23.
Mayo, Keenan, and Newcomb, Peter. “How the Web Was Won: An Oral History of the Internet.” *Vanity Fair,* July 2008.
Nakashima, Ellen. “Hackers Breach Some White House Computers.” *The Washington Post*, October 28, 2014.
———. “NSA Allies with Internet Carriers to Thwart Cyber Attacks against Defense Firms.” *The Washington Post*, June 7, 2011.
Nakashima, Ellen, and William Wan. “U.S. Announces First Charges against Foreign Country in Connection with Cyberspying.” *The Washington Post*, May 19, 2014.
Nicholson, Jessica, and Ryan Noonan. “Measuring Bytes across Borders | Economics and Statistics Administration,” January 27, 2014.
Nunes, Devin. “H.R.1560 - 114th Congress (2015-2016): Protecting Cyber Networks Act.” Legislation, April 27, 2015.
Nye, Joseph S. Professor, Harvard University. Personal Interview, December 1, 2014.
Obama, Barack H. “Foreign Policy Cyber Security.” *The White House*. Accessed February 28, 2015.
———. “Remarks by the President at the Cybersecurity and Consumer Protection Summit.” *The White House*.
Pals, Fred, and David Voreacos. “Accused Russian Hacker May Be in U.S. Hands Soon.” *Bloomberg*, November 4, 2014.
Paul, T. V., Patrick M. Morgan, and James J. Wirtz. *Complex Deterrence : Strategy in the Global Age*. Chicago: University of Chicago Press, 2009.
Pellerin, Cheryl. “Rogers: Cybercom Defending Networks, Nation.” *Defense.gov News*, August 18, 2014.
Perera, David. “DoD Enacts Rule on Excluding Contractors Based on Supply Chain Risk.” *FierceGovernmentIT*.

Perlroth, Nicole. “Anonymous Hackers’ Efforts to Identify Ferguson Police Officer Create Turmoil.” *The New York Times*, August 14, 2014.
———. “Hacked vs. Hackers: Game On.” *Bits Blog*, December 2, 2014.
Perlroth, Nicole, and David E. Sanger. “North Korea Loses Its Link to the Internet.” *The New York Times*, December 22, 2014.
Ponemon Institute Research Report. *2013 Cost of Cyber Crime Study*. HP Enterprise Security, October 2013.
“Presidential Policy Directive -- Critical Infrastructure Security and Resilience.” *The White House*.
“Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).” Department of Defense, November 5, 2012. DoD Instruction 5200.44.
Purcell, Kristen. *Search and Email Still Top the List of Most Popular Online Activities*. Pew Internet & American Life Project. Pew Research Center, August 9, 2011.
Quinn, Richard P. “The FBI’s Role in Cyber Security.” Statement Before the House Homeland Security Committee, Subcommittee on Cyber Security, Infrastructure Protection, and Security Technologies, Washington, D.C., April 16, 2014.
Rehman, Scheherazade. “Estonia’s Lessons in Cyberwarfare.” *US News & World Report*, January 14, 2013.
Reuters. “U.S. State Department Email System Reportedly Hacked.” *The Huffington Post*, November 17, 2014.
Reveron, Derek S. *Exporting Security : International Engagement, Security Cooperation, and the Changing Face of the U.S. Military*. Washington, DC: Georgetown University Press, 2010.
Riley, Michael. “China Mafia-Style Hack Attack Drives California Firm to Brink.” *Bloomberg*, November 27, 2012.
Robb, David. “Sony Hack: A Timeline.” *Deadline*, December 22, 2014.
Sanger, David. Personal Interview, November 4, 2014.
Sanger, David E., and Martin Fackler. “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say.” *The New York Times*, January 18, 2015.
Sanger, David E., and Michael S. Schmidt. “More Sanctions on North Korea After Sony Case.” *The New York Times*, January 2, 2015.
Sanger, David E., Thom Shanker, and John Markoff. “In Digital Combat, U.S. Finds No Easy Deterrent.” *The New York Times*, January 26, 2010, sec. World.
Schelling, Thomas C. *Arms and Influence*. New Haven, Yale University Press, 1966.
Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations.* Penguin Book, 2008.
Shirky, Clay. “The Political Power of Social Media.” *Foreign Affairs*, no. January/February 2011 (February 2011).
Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, 2014.
Son, Hugh. “Dimon Sees Cyber-Security Spending Doubling After Hack.” *Bloomberg.com*, October 10, 2014.
Sternstein, Aliya. “Fallout from Clinton’s Private Emails: How Secure Are Agency Email Systems?” *Nextgov.com*, March 5, 2015.
Stokes, Bruce. “Extremists, Cyber-Attacks Top Americans’ Security Threat List.” *Pew Research Center*. Accessed February 26, 2015.

Theohary, Catherine A., and John W. Rollins. “Cyberwarfare and Cyberterrorism: In Brief.” *Congressional Research Service*, no. R43955 (March 27, 2015): 12.
“Top 10 Uses of Internet.” *Before It’s News | Alternative News | UFO | Beyond Science | True News| Prophecy News | People Powered News*, June 22, 2013.
“U.S. Defense Chief Warns of Digital 9/11,” October 11, 2012.
Weldon, David. “Thwarting a New Breed of Cyberattack.” *FierceCIO*, January 27, 2015.
Williams, Dean. *Leadership for a Fractured World : How to Cross Boundaries, Build Bridges, and Lead Change*. First edition. San Francisco: Berrett-Koehler Publishers, 2015, 2015.
Zind, Steve. “GlobalFoundries Purchase Of IBM Essex Prompts Security Review,” November 2, 2014.