Cyber Warfare: Changing the Reality of Warfare Capabilities in the 21st Century

By Alexander Kolodner
Tufts University '14

Table of Contents

INTRODUCTION

Cyber Warfare. Such an ominous sounding word has been flashed in headlines for years as a warning of things to come. Yet, for all the warnings and thousands of articles published there has yet to be a true manifestation

The following work is a condensation of thousands of pages and research in the field of cyber warfare. In order to actually begin speaking about cyber warfare I often find there are a lot of misunderstandings surrounding the different impressions and interpretations about what "cyber warfare". Many people believe it to be the end all of warfare, others interpret it in a more clausewitzian "extension of politics" fashion. Ultimately, I interpret cyber warfare to be the simple expansion of war into a new domain.

Some of the major questions that surround the study of cyber warfare are:

What if you could eliminate your enemy without having to kill anyone? Without having to even leave the comfort of your living room? How do troops organize in cyberspace? How does a state resolve attribution when an attack does not necessarily reveal the attacker? What is the impact on cyber war for troop morale? Which Americans are most at risk in the event of a cyber war? What are the United States' most vulnerable points? How can those vulnerable points be made stronger?

These are the questions that every state must ask itself and be prepared to answer.

One major theme that runs throughout the thesis is the idea that entities become more alike to their enemies the longer the conflict occurs. As I will demonstrate throughout my thesis, the tools and tactics used by the United States and its allies become more similar to its enemies and are now at the point where state and non-state actors appear deceivingly similar in cyberspace.

In my thesis, I will begin with an overview of the United States' cyber warfare capabilities. I will then discuss the various actors involved in cyber war and discuss their various capabilities. I will then turn the lens back on the United States and examine the creation of a cyber military industrial complex as well as critique possible political blowback from cyber policies. Finally, I will offer my own recommendations

as to how the United States can improve its cyber war efforts in order to create a better defensive structure and operate more efficiently from an international relations perspective.

CHAPTER 1: WHAT IS CYBER WARFARE?

"…it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country."[1] – President Barack Obama

The United States is the strongest military power humanity has ever seen. The missiles, tanks, aircraft carriers, fighter jets, drones, and small arms paired with a robust economy have all contributed to U.S. military domination throughout the 20th century. As humanity stumbles and falls into the 21st century, warfare is taking on a new format, or rather, a return to an old format. For the past 400 years, states have largely waged war between themselves. However, war-making capabilities are slipping back into the hands of the non-states. The rise of organized non-state fighters like Al Qaeda, Hezbollah, and the Taliban are indicative of a larger shift in war making capabilities.

As the balance of power tilts and shifts, virtually all parties are looking to new technology to gain an advantage in war. With the rise of and spread of the Internet, those that seek to use it to do harm are capitalizing on its inherent design flaws in order to carry out unprecedented attacks. This new type of warfare is called cyber warfare and it is poised to drastically shape international relations for the 21st century. Both states and non-state are looking to the Internet as the universal toolbox, capable of a multiplicity of tasks, one of which is warfare.

In order to clarify a series of terms and lay a framework for understanding the various components of cyberspace, I will spend this chapter analyzing the common definition of cyber warfare. I will then introduce an alternative, more precise definition with an accompanying framework for cataloging various types of cyber attacks. There are many misconceptions surrounding the terminology cyber warfare. The framework I provide will help to clarify those misconceptions and also help to provide context for an appropriate response. Finally, I will explain why old-war terms, such as victory and defeat, cannot be seamlessly recast to reflect new-war realities.

---

[1] Barack, Obama. 2009. "Remarks by the President on Securing Our Nation's Cyber Infrastructure". Speech May 29, The White House, East Room. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

The term cyber warfare carries a slightly different meaning depending on state terminology. In China, cyber warfare is replaced by the broader term "Information Warfare" that includes "the enemy's information detection sources, information channels, and information-processing and decision making systems."[2] Within the United States, the media, military, and academic fields tend to gravitate towards the term cyber warfare to describe a wide range of activities. However, the indiscriminate use of the term by each field continues to fuel widespread ambiguity of the term. Whereas information warfare has relatively precise actions, cyber warfare remains relatively broad and ambiguous.

Since western media tends to use an overly vague term to define cyber warfare, the first definition of cyber warfare is the very general and commonly understood term for a battle between two groups that exists solely in cyber space. In 2013, the hacker-collective Anonymous threatened Indonesian hackers "that if they do not stop infiltrating private Aussie web sites the two factions could engage in an all-out cyber-war."[3] However, the scale of warfare to which the hackers are referring is hardly on the scope of true cyber warfare. Colloquial use of the term war is often used to hyperbolize events that do not actually meet the threshold for "war". For example, FOX News often uses the term "War on Religion" to describe the treatment of Christians in U.S. culture.[4] Be that as it may, when viewed through the context of war studies it is clear that no such war exists. When the term cyber warfare is used in the same colloquial context it adopts the same hyperbolized context as in the term "War on Religion".

The hyperbolized type of cyber warfare generally involves attacking a few websites that then get brought back online within a week. Total damage from the attacks is minimal and hardly noticeable on a global scale. This definition of cyber warfare tends to be used by those people that are unfamiliar with the parameters that surround warfare.

---

[2] Zhang Yuliang, ed. Zhanyi Xue (The Science of Military Campaigns), Beijing, China: National Defense University Press, 2006, p.155, quoted in "The Chinese People's Liberation Army and Information Warfare", Wortzel, Larry M.

[3] "Anonymous Factions Threaten Cyber-War on One Another over Anti-NSA Hacks." 2013. *RT*. November 11. http://rt.com/news/anonymous-factions-cyber-war-australia-564/.

[4] Shackelford, Kelly. 2013. "Yes, Virginia, There Really Is a War on Christmas". News. *FoxNews.com*. December 17. http://www.foxnews.com/opinion/2013/12/17/yes-virginia-there-reall-is-war-on-christmas/.

A clearer definition offered by Susan Keating sheds some well-needed light onto the boundaries of true cyber warfare. Keating explains, "…cyberwar is an attack that uses computer networks in an attempt to disable anything from a single business to an entire society...Targets include government, military, industry and infrastructure."[5] Keating's explanation helps to provide a preliminary framework for discussing cyber warfare. However, the definition lacks a set a threshold of harm, does not factor in the rational for an attack, nor does it explain the various actors and the degree to which those actors influence the intensity of the cyber war. Additionally, the definition wrongfully narrows down the title of warfare to only a single attack.

In an effort to better categorize the various types of cyber attacks, I have developed a three-part framework to more accurately identify true cyber warfare. To date, there have been no such cases of a "pure" cyber war (one that exists purely in cyber space). The following framework will help delineate between various types of cyber conflicts.

With the expansion of cyber actors and resources, the ability to wage war has transformed from a Clausewitzian conception of war by allowing non-state actors to be able to engage in acts of war. However, in cyber warfare it is too easy to shroud one's identity. Therefore, the first qualification is that cyber warfare can only be waged between at least two identifiable entities, either state or non-state. The first requirement is critical for eliminating the possibility of a war akin to the War on Terror launched by the Bush Administration in 2001. Fighting a war against an idea in cyberspace would be incredibly unproductive as cyberspace is not a static object, but rather it is an ever evolving and flowing existence. Attempting to launch a concentrated war effort against bodies that always move proves to be excessively cost prohibitive and unproductive. Additionally, resolving cyber identities to physical world identities is technically difficult and time consuming.

In his book, *America the Vulnerable*, Joel Brenner explains one of the misgivings of the U.S. to declare any sort of cyber war saying, "When you declare war, you must declare it against somebody

[5] Keating, Susan. 2013. "The Cyber Fight." *The Guard Experience*. November 21. http://gxonline.com/features/cyber-fight.

specific."[6] The inability to accurately attribute the source of an attack complicates the ability of states to declare war in cyberspace, thus the need for the first requirement.

The second qualification is that the state or non-state entity must have an identifiable agenda for carrying out the attack that includes political, economical, technological, or moral advancement. Intentions that are proven to be irrelevant to standard warfare ideology will not be classified as cyber warfare and instead regulated to a lesser cyber event such as a skirmish or standard attack. Modern warfare is clouded in ideology and political, economic, or moral motivations. War theorist and historian, Mary Kaldor, deduces in her book *New and Old Wars* that 21st century warfare is mobilized on ideological lines.[7] In order to convince the American public to enter Iraq, former President Bush argued that the United States had a responsibility to spread freedom and democracy to every nation.[8] Later revelations revealed the ascertainment of key oil resources to be a central motivation for going to war.[9] Wars may still be fought for resources, but they are certainly sold to the public based on ideological imperatives.

Cyber attacks are launched for dozens of reasons, some of which are not characteristic of ideologies and are instead fueled by non-political intellectual challenges. One hacktivist group, LulzSec, defaced websites and penetrated secure servers for non-political, non-moral reasons over a period of several months in 2011. The group traversed the Internet shaming organizations claiming to be security experts by defacing their websites and releasing their personal information online. LulzSec left untouched the ample opportunities for financial gain. Because of the relative intensity and longevity of the attacks, the group dances a fine line between cyber skirmishes (to be discussed later) and cyber warfare. Yet, once the underlying motivation of shaming security is factored into the equation, it is obvious that LulzSec's

---

[6] Brenner, Joel. 2011. *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press. Pg 129.
[7] Kaldor, Mary. 2007. *New and Old Wars: Organized Violence in a Global Era, Second Edition*. 2nd Edition. Stanford, Calif.: Stanford University Press. Pg 16.
[8] Reynolds, Maura. 2003. "Bush Says U.S. Must Spread Democracy." *Baltimoresun.com*. November 7. http://www.baltimoresun.com/news/bal-te.bush07nov07,0,5347312.story.
[9] Juhasz, Antonia. 2013. "Why the War in Iraq Was Fought for Big Oil." *CNN*. April 15. http://www.cnn.com/2013/03/19/opinion/iraq-war-oil-juhasz/index.html.

activities cannot be classified under any conception of cyber warfare. I will discuss LulzSec more in chapter 2.

The final requirement, and perhaps the most important, is that the cyber attacks must also reach a threshold of harm to be classified as an act of cyber warfare. Harm can include economic, political, or technological as well as possible kinetic damage. Testifying before the U.S. Congress, the former head of NSA/CSS, General Keith Alexander revealed that there are thousands of cyber attacks launched against the United States government and companies everyday.[10] The United States would be at a total loss if it were to classify each one of the attacks as an act of war, especially when considering most of the daily attacks are largely insignificant and fruitless. Instead, cyber attacks must reach a threshold of harm in order to even be considered as a possible act of cyber warfare thereby limiting the framework of the discussion to a manageable degree.

The next logical question becomes, what is threshold for an attack?
Many cyber experts have difficulty in creating a threshold because there simply is no standard from which to create a threshold.[11] I believe the threshold should not be a static point but rather a range of different possibilities decided on a case-by-case basis. If a member of Al Qaeda kills two civilians in a random occurrence, should that attack be considered as an act of war? Probably not. But what if organized members of Al Qaeda take over a mall and systematically kill customers? Is that an act of war? And to extend this analogy one step further what if the head of Al Qaeda issues a command to attack the United States and organizes 19 individuals to fly planes into major U.S. infrastructure. Have we now surpassed the threshold for what constitutes an act of war?

In order for an attack to be considered as part of an overarching cyber war the attack must surpass a flexible threshold, namely, the attack must be successful enough to even be considered beyond

[10] DeWalt, David. "Threat and Response: Combating Advanced Attacks and Cyber-Espionage Keynotes". Speech Center for Strategic and International Studies.
[11] Joel Brenner, Peter Singer, and Richard Clarke explicitly do not lay out a threshold in each of their respective books.

the thousands of attacks that occur daily. The attack must successfully penetrate the intended target and be recognized by the victim as an attack and not simply a glitch or program error.

One of the complexities in creating a set threshold is the need to factor in the respective power of each state or non-sate involved in the cyber war. States are notorious for being able to bend the rules regarding attacks. Take for example, the United States' recent drone strikes into Pakistan. Pakistan, though upset, has yet to declare war against the United States for such attacks. Similarly, the United States has launched several sophisticated cyber attacks including Duqu, Flame, and Stuxnet against Iran. Certainly the attacks have been successful and penetrated the Iranian infrastructure. Yet, Iran has yet to declare war on the United States as a result of the cyber attacks. When deciding a set threshold for when a cyber attack (or series of attacks) meets a given threshold, it is paramount to also consider the power dynamics of all parties involved. Most importantly, even if a threshold is met, it does not mean war must be declared, only that the option is now available.

In addition to full-scale cyber warfare, there are two stages of intensity that function as subsets leading to full out cyber war. The first level is that of a simple cyber attack. A cyber attack includes the credit card scams, phishing attacks, malicious emails, messages, and websites that overwhelmingly populate cyber space. Some of these attacks can be more complex but a large majority of the attacks are ineffective attempts at financial gain or espionage.

Also under the first classification of cyber attack is the term cyber operations. Cyber operations is a broadly used definition created by the U.S. intelligence community to describe any sort of cyber activity. Specifically:

> U.S. agencies define offensive cyber-operations as activities intended "to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves," according to a presidential directive issued in October 2012.[12]

[12] Gellman, Barton, and Ellen Nakashima. 2013. "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show." *The Washington Post*, September 3, sec. World. http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

Because of its breadth, the term cyber operation is primarily used to separate events that occur in the cyber world from events that occur in the physical world. A cyber operation can be anything from spying on a target via the Internet to launching a full out cyber attack. Moving beyond the first classification is the slightly more complicated cyber espionage.

Cyber espionage is the adaptation of traditional espionage into cyber space. It includes obtaining trade secretes, intellectual property, insider information, or even military schematics in order to then sell that information on the black market or use for political gain. After gaining entry to the network, an attacker siphons documents and information out of the victim's network. Both states and non-states engage in cyber espionage, the most notorious of which are the Chinese (both state actors and non-state actors).

In 2003, the United States Department of Defense noticed a massive amount of data being transferred away from its unclassified network, NIPRNET, towards an IP address located in China. The DoD could not identify the exact information that was being copied but was able to provide a list of departments including the "Defense Information Systems Agency, the Redstone Arsenal, the Army Space and Strategic Defense Command, and several computer systems critical to military logistics."[13] The leak is the largest theft of U.S. defense networks totaling between 10 and 20 terabytes of data stolen. By no coincidence, the Chinese military has developed key pieces of technology that directly mirror American-developed technology. Specifically the Chinese military copied a "quiet electric drive for its submarines and ships so they'd be silent and hard to track" as well as a "new radar for their top-of-the-line Aegis Cruiser."[14] The attack has been rightfully titled, Titan Rain.

Yet, Titan Rain was not the first time the DoD's infrastructure had been extensively penetrated. In 1998 and in 2001 hackers penetrated the DoD's cyber infrastructure in order to siphon critical information related to "...U.S. agencies such as the DOE and NASA, as well as from military contractors

---

[13] Brenner, Joel. 2011. *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press. Pg 116.

[14] Clarke, Richard A., and Robert Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It*. Reprint edition. New York: Ecco. Pg 12.

and universities."[15] The United States may be the most sophisticated cyber actor on the planet, but that has not left us invulnerable to successful attacks.

Cyber espionage is reported by the Center for Strategic and International Studies to cost the U.S. between $70 billion and $280 billion a year.[16] Other estimates put that number well into the trillions if you factor in the additional consequences of an attack such as loss of contracts.[17]

In addition to the costs of the actual attack, there can be additional monetary damages imposed that increase the overall cost of espionage. In 2006, a thief broke into an employee of the VA's private residence and stole his government issued laptop. The laptop contained confidential information on 26.5 million active duty troops and veterans. The police eventually found the thief and the laptop, but as a result of the risk created by the theft, five groups representing veterans filed a class actions lawsuit against the VA. The VA settled in 2009 to a total of $20 million for damages.[18] Stealing a laptop with confidential information is an extension of cyber espionage through its incorporation of both physical and cyber elements.

Another form of indirect costs stems from how the companies compete on an international level. American companies and military agencies incur additional costs when they lose key intelligence to foreign companies, thereby forfeiting their competitive edge. The difficulty of finding the source of the attack also lends itself to create a fertile environment for cyber espionage as skilled attackers can continue their attacks with minimal fear of being caught.

The primary difference between cyber espionage and cyber warfare is that cyber war is conducted for ideological or geo-political reasons while cyber espionage primarily targets economic roots or

---

[15] Shackelford, Scott. 2009. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (1): 191–250. Pg 204.
[16] "The Economic Impact of Cybercrime and Cyber Espionage." 2013. Center for Strategic and International Studies. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf. Pg 4.
[17] DeWalt, David. "Threat and Response:Combating Advanced Attacks and Cyber-Espionage Keynotes". Speech Center for Strategic and International Studies.
[18] Frieden, Terry. 2009. "VA Will Pay $20 Million To Settle Lawsuit Over Stolen Laptop's Data." *CNN*, January 27. http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/.

information sources. I will speak more on the differentiation of cyber warfare versus traditional warfare in later chapters.

The second stage leading to all out cyber warfare is a cyber skirmish. A cyber skirmish is a transfer of the qualities of a real-world skirmish into the cyber world. A cyber skirmish distinguishes itself from a single attack because it includes either repeated assault by the attacker or retaliation from the victim. Unlike cyber espionage, a cyber skirmish ignores possible economic or technological gain from attacks and is instead focused on causing harm (whether economic, political, or ideological) to the target.

In 2008, in response to Israeli Operation Cast Lead, Palestinian hackers joined forces to deface Israeli websites as a form of protest. The attacks featured both state and non-state hackers who targeted both private and public websites. The rapidity with which each side launched attacks at the opposing side rightly fits the definition of a cyber skirmish. Each side did not specifically know the actors on the other side of the conflict. This cyber skirmish does not meet the first or third qualification for cyber warfare. The attackers were not explicitly known and the harm was relatively minor.

Throughout the Syrian revolution, the Syrian Electronic Army (SEA), a pro-Assad collective of hackers, launched a series of cyber attacks against Western governments, news outlets, and businesses. In 2014, the European Electronic Army (EEA) launched a series of retaliatory attacks against pro-Assad Syrian websites and cyber infrastructure, ultimately claiming credit for briefly shutting off Syria's entire Internet access. As of spring 2014, the two collectives continue to launch repeated attacks against each other in perfect demonstration of a cyber skirmish.

Which group is "winning" the skirmish between the SEA and EEA? The old-war mentality of victory and defeat has difficulty being transferred into cyber space. Victory is not a clearly defined end point for cyber actors. Does victory mean total submission of enemy forces? Does victory mean financial gain for the victors? Does victory mean the ascertainment of critical intelligence?

William Martel, professor at the Fletcher School of Law and Diplomacy, writes about the theory of victory in war, first defining it in military terms and then political terms saying:

> The word victory, which derives from the Latin victoria…is defined in military terms as 'Defeat of an enemy in battle, of or an antagonist in any contest' and in political terms as 'gaining…the superiority of success in any struggle or competition.'[19]

These two standard conceptions of victory fail to embrace the dynamic field of cyber warfare because of the complexity of different motivations and possibilities. Attacks can be launched for a variety of reasons, many of which do not include political gain.

In order to understand both the complexities of cyberspace and accurately critique the impact of cyber warfare, it is first necessary to investigate the different actors operating in cyberspace – namely the state and the non-state actors. In the next chapter I will introduce the various actors operating in cyber space.

[19] Martel, William. 2012. *Victory in War: Foundations of Modern Strategy*. 2nd ed. Cambridge; New York: Cambridge University Press. http://www.amazon.com/Victory-War-Foundations-Modern-Strategy/dp/0511842449/ref=sr_1_3?ie=UTF8&qid=1398026773&sr=8-3&keywords=victory+in+war+martel. Pg 21.

CHAPTER 2: WHAT PARTIES ARE INVOLVED IN CYBER WARFARE?

As of 2012, there are almost 2 billion people navigating the World Wide Web.[20] By 2020 that number is expected to more than double.[21] More people active on the Internet could open up new channels for communication across cultures that have never spoken with each other. Yet, more people on the Internet can also mean a greater number of cyber threats as the cost of entry of developing a cyber weapon plummets. How the United States confronts these multiple upcoming challenges will undoubtedly decide its strategic military power for the ongoing century.

In this chapter I will review the major state and non-state cyber actors and provide insight into several of their respective technical abilities in relation to the United States' own abilities. I will then detail the role that non-state actors have in the cyber world and catalogue the various non-state actors into three major categories.

There are over a hundred states with active cyber programs.[22] These programs vary in overall effectiveness, intent, level of development, and funding. Some programs, like France's or Germany's, are in the preliminary stages of development and are primarily used for information reconnaissance. Other programs, like China's or Russia's, are very advanced and capable of carrying out major cyber campaigns. A majority of states have not had to use any cyber offensive capabilities as of yet, though a few have launched very sophisticated cyber attacks, which I will discuss later.[23]

---

[20] Gross, Doug. 2013. "Google Boss: Entire World Will Be Online by 2020." *CNN*. April 15. http://www.cnn.com/2013/04/15/tech/web/eric-schmidt-internet/index.html.
[21] Ibid.
[22] Brenner, Joel. 2011. *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press. Pg 73.
[23] "Germany Reveals Offensive Cyberwarfare Capability." 2012. *Atlantic Council*. June 8. http://www.atlanticcouncil.org/blogs/natosource/germany-reveals-offensive-cyberwarfare-capability.

Despite the myriad of programs, talk of cyber warfare often centers on the big three - the United States, China, and Russia. Each of these states has strengths that distinguish it from other states and each of these states has launched a major cyber offensive against another state. As of currently, the U.S. is widely regarded by cyber warfare experts as the top country capable of carrying out the most impactful cyber attacks.[24]

The United States earned its dominance through massive prolonged military spending and research into cyber infrastructure and development. The U.S. has unprecedented forces working in both the public and private sector for the reinforcement and study of target infiltration and attack methods. The United States heavily relies on defense contractors to develop cyber weapons and cyber defenses. I will discuss more on this topic in chapter 4.

Despite the United States' offensive capabilities, some defense scholars, such as Richard Clarke, believe China to be the most capable of defending itself from cyber attacks because of its focus on infrastructure security.[25] China has designed its physical network to have the capability to isolate itself from any outside signals. In the case of a severe cyber attack, China could isolate its cyber infrastructure from the rest of the world. The network can then be subdivided into micro-networks for further protection. Even if an attack originated from within the state, it could only extend as far as its specific micro-network.

Based on China's current capabilities and past actions, the United States should expect continued attacks against U.S. intelligence communities and U.S. efforts. President Obama has met with President Xin Jinping several times to discuss the ongoing cyber exchange between the United States and China. Recent revelations by Edward Snowden of U.S. cyber programs against Chinese companies and agencies have fueled the ongoing tension between the two states.

The third major player is Russia. Russia has two strong arms that enable it to launch major attacks. The first arm is Russia's government investments into cyber capabilities and the second arm is

[24] In terms of physical, economic, and socio-political damage potential.
[25] Clarke, Richard A., and Robert Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It*. Reprint edition. New York: Ecco. Pg 148.

Russia's support of pro-Russian hacker groups. In three scenarios within the last ten years Russia has accompanied ground invasion with a coordinated cyber attack. Before and during the invasion in Estonia, Georgia, and Crimea, Russia launched major cyber attacks in order to eliminate communication among top officials and induce a virtual fog-of-war.[26] [27] The third attack used in Crimea is slightly different from its predecessors because Russian troops physically shut down the communication channels, but still remains well within the field of a cyber operation.

In February of 2014, G-Data, a German anti-virus company, uncovered the existence of the Uroburos rootkit.[28] Uroburos infects a computer and then sends information back to a central server. The piece of malware is especially impressive because it does not rely on the computer to be connected to the Internet in order to relay information back to the central source. Instead, a computer that is not connected to the Internet but is infected with the virus can transfer information through an infected computer back to the server.[29] For example, devices such as laptops are often used on the Internet and smaller Intranets. As a laptop physically travels between the two networks, it can collect, temporarily store, and then transfer information back to the server. Based on both the technical level of the attack along with clues from the underlying language used in the malware's programming, researchers believe Russian cyber forces created the malware. The most surprising part is that the malware is built into a piece of software created in 2011, meaning the intrusion had been active for at least 3 years before being discovered. This kind of sophisticated attack places it within the same category as Stuxnet and Flame. The attack is not part of a larger war or skirmish; therefore, the attack is better categorized as cyber espionage created by the Russian state.

---

[26] Boyle, Jon. 2014. "Ukraine Hit by Cyberattacks: Head of Ukraine Security Service." *Reuters*, March 4. http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-telecoms-idUSBREA230Q920140304.
[27] Harris, Shane. 2014. "Hack Attack - Russia's First Targets In Ukraine: Its Cell Phones and Internet Lines." *Foreign Policy*, March 3. http://www.foreignpolicy.com/articles/2014/03/03/hack_attack.
[28] "Uroburos - Highly Complex Espionage Software With Russian Roots." 2014. Blog. *Security Blog*. http://blog.gdatasoftware.com/blog/article/uroburos-highly-complex-espionage-software-with-russian-roots.html.
[29] Cluley, Graham. 2014. "Anti-Virus Firm Finds Alleged Kremlin Cyberweapon, Undetected for at Least Three Years." *Graham Cluley*. Accessed April 20. http://grahamcluley.com/2014/03/russian-spyware/.

Besides the big three, most states have some sort of cyber program with varying degrees of development. Programs like France's have yet to be officially used whereas Israel is thought to have contributed towards two major cyber attacks; one against Iran, and one against Syria.[30] Germany announced in 2012 that its cyber program has the capabilities to launch major offensive cyber strikes if necessary.[31] An April 2014 report from the Australian Strategic Policy Institute ranked Australia as the third most prepared state for cyber warfare in the Asia Pacific region preceded by China ranked second and the United States ranked first. Australia is followed by Singapore and South Korea with North Korea ranked dead last.[32]

Besides the states, many non-state actors are active in the cyber domain. Moving into the 21st century, non-state actors are becoming significantly more powerful on an international scale. General Keith Alexander brought the issue of strengthening non-state actors to light in an interview with the Center for Strategic and International Studies remarking, "More people were killed in 9/11 than in Pearl Harbor."[33]

In the 2011 U.S. National Military Strategy Report delivered by Admiral M. G. Mullen, he explains the growth of non-state actors saying, "State-sponsored and non-state actors complicate deterrence and accountability by extending their reach through advanced technologies that were once solely the domain of states."[34] Non-state actors have gained control of powerful forces both physical and cyber. In some cases those non-state actors were actually armed by the United States. For example, in

---

[30] Markoff, John. 2010. "A Silent Attack, but Not a Subtle One." *The New York Times*, September 26, sec. Technology. http://www.nytimes.com/2010/09/27/technology/27virus.html.
[31] Fischer, Michael, Joerg Blank, and Christoph Dernbach. "Germany Confirms Existence of Operational Cyberwarfare Unit." *Deutsche Presse-Agentur*. June 5, 2012. es.com/news/germany-confirms-existence-of-operational-cyberwarfare-unit-1.179655.
[32] Yenko, Athena. 2014. "Will Australia Launch Cyber War Soon?" *International Business Times*. April 15. http://au.ibtimes.com/articles/548171/20140415/cyber-war-australia-strategic-policy-institute.htm.
[33] Zheng, Denise. 2010. "Interview with General Keith B. Alexander, Director of the NSA and Commander, Cyber Command" iTunes University.
[34] Mullen, M. G. 2011. "The National Military Strategy of The United States of America". Government Report. Washington, D.C. http://www.army.mil/info/references/docs/NMS%20FEB%202011.pdf. Pg 4.

2014, the U.S. Congress voted behind closed doors to provide small arms to Syrian rebels.[35] In the future, the United States could also consider providing rebels key cyber tools to fuel their efforts.

Non-state actors can best be understood and combatted by first understanding their motivation for organizing. In order to better understand each type of non-state group, I have separated the various types of non-state actors into easily identifiable sub categories. By separating the types of non-state actors the patterns governing actions, capabilities, and ways to neutralize each group can be realized and implemented. The following table provides an easy reference for each type of non-state actor as well as common state actors.

The Relationship Between State and Non-State Actors and Their Motivations for Launching an Attack

	Political Intentions	**Ideological Imperatives**	**Non-Political, Non-Moral Reasons**
State	China, Russia, U.S., Israel, Australia.		
Non-State	Hidden Lynx, European Electronic Army.	Anonymous, Al Qaeda, European Electronic Army, Team Hell, Team Evil.	Anonymous, LulzSec, Chinese Human Flesh Search Engine.
State Coordination of Non-State Actors	**First Compartment**: China, Russia, LulzSec, Syrian Electronic Army.		
Nonstate actors working apart from the state but towards similar goals	**Third Compartment:** Hidden Lynx, Russian Estonia Hackers, (Cyber Berkut, Team Evil, Team Hell, Jurm Team, C-H Team, Hackers Pal, Gaza Hacker Team, DNS Team, !TeAm RaBaT-SaLe!, DZ Team, Ashianeh Security Group, Nimr al-Iraq.)	**Second Compartment**: Syrian Electronic Army, Anonymous, (Cyber Berkut, Team Evil, Team Hell, Jurm Team, C-H Team, Hackers Pal, Gaza Hacker Team, DNS Team, !TeAm RaBaT-SaLe!, DZ Team, Ashianeh Security Group, Nimr al-Iraq.)	

[35] Hosenball, Mark. 2014. "Congress Secretly Approves U.S. Weapons Flow To 'Moderate' Syrian Rebels." *Reuters*, January 27. http://uk.reuters.com/article/2014/01/27/us-usa-syria-rebels-idUKBREA0Q1S320140127.

Within the chart I have included several groups as part of multiple different categories. Many of these groups went through transformative periods in which their identity and purpose evolve and therefore they can be classified by multiple possible identities based on different points in time. This chart is by no means representative of the entirety of cyber actors because many attacks are launched without announcing the source of the attacks.

Some cells are intentionally left blank because those types of groups do not exist. For example, states do not carry out attacks that are not somehow inherently political. Similarly, states do not coordinate the actions of non-states for reasons that are not political.

The first compartment is made up of non-state actors that work as an extension of the state. The second compartment is made up of non-state actors that operate out of a sense of patriotism or nationalism and do so without the cooperation or organization of the state. The third compartment is composed of non-state actors that operate out of a commitment to ideology.

China and Russia have strong ties with non-state actors that work in combination with state efforts to launch sophisticated cyber attacks.[36] The PLA hosts hacking competitions to recruit cyber soldiers. In one such case, the winner of the competition was caught hacking Japanese websites, recruited by the PLA, offered additional training by the PLA, and later caught hacking into the Pentagon.[37] China claimed he was acting independently. Cases like this highlight state involvement in the production and training of state sponsored hackers.

In January of 2013, Chinese hackers gained access to "some two dozen of America's most advanced weapons systems."[38] As per usual, it is nearly impossible to tell if the attacks were state

[36] Demchak, Chris C., and Peter Dombrowski. 2011. "Rise of a Cybered Westphalian Age". DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA537560.
[37] Kelly, Mary Louise. 2010. "Cyberwarrior Shortage Threatens U.S. Security." *NPR.org*. NPR. http://www.npr.org/templates/story/story.php?storyId=128574055.
[38] Keating, Susan. 2013. "The Cyber Fight." *The Guard Experience*. November 21. http://gxonline.com/features/cyber-fight.

sponsored or were the workings of non-state actors. More likely, it was non-state actors working for hire by the Chinese government because of the sophistication of the attack and the nature of the target. The information included "the Patriot missile system, the Navy's Aegis ballistic missile defense system, the F/A-18 jet, the V-22 Osprey aircraft, the Black Hawk helicopter, and the F-35 Joint Strike Fighter."[39] The schematics of these weapons systems form some of the core weapons systems of the United States military. The UH-60 Black Hawk helicopter and its variants is one of the most widely used U.S. Army helicopters. Being able to replicate its specific designs and identify its weaknesses posses a potentially serious problem to U.S. military dominance. This example is yet another instance of the multiplicity of cyber espionage cases yet remains distinctly outside the realms of cyber warfare.

States benefit legally from working with non-state actors because the country can pass off blame for an attack to a rogue actor. China can pass off responsibility for the actions of its non-state actors while still receiving all the benefits from the stolen information.

The United States has some of the most powerful cyber infrastructure in the world. Despite this infrastructure, the United States still benefits from working with non-state actors. Non-state actors allow for the U.S. to carry out attacks would not have normally been an option.

In 2011, LulzSec ran rampant through the Internet hacking and defacing websites as they pleased.[40] LulzSec was strongly anti-government and categorically rejected the unfettered surveillance of Internet communities by federal agencies. After successfully hacking Sony, Senate.gov, CIA.gov, the *Times*, *The Sun*, and several other companies and government sites, the group was eventually rounded up and arrested.

LulzSec was structured around a central leader, Sabu, who would provide targets for the members. During the trial of one of the groups' members, it came to light that Sabu was receiving his targets from FBI informants. Sabu would then pass those targets along to the group who would then conduct the attack.

---

[39] Ibid.
[40] Olson, Parmy. 2013. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Reprint edition. New York: Back Bay Books.

Jeremy Hammond, former hacker working alongside Sabu, explains the process of picking targets saying, "'Sabu' had supplied him with lists of websites that were vulnerable to attack, including those of many foreign countries."[41] By this time in the hacking spree Sabu's physical world identity, Hector Xavier Monsegur, had been discovered by the FBI. In order to avoid jail time, Monsegur agreed to become an informant and help discover the identities of the other members of LulzSec.

Of the servers on the list, "[Hammond] mentioned specifically Brazil, Iran and Turkey before being stopped by judge Loretta Preska, who had ruled previously that the names of all the countries involved should be redacted to retain their secrecy."[42] Hammond's testimony supports the notion that the United States tricked the LulzSec into doing some of its dirty work while passing off blame to the delinquent group. Thus, in the previous chart I have classified LulzSec as both a non-state actor working for fun for their earlier attacks and as a non-state actor coordinated by the state for their later attacks.

The idea that LulzSec was used to carry out some of the United States' dirty work is further supported by fact that Hammond was not charged with hacking the websites of foreign nations. He was instead charged with his original attack of Strategic Forecasting, Inc, a domestic private intelligence company. The attacks that were recorded and setup by the FBI never became part of the sentence. Some questions remain unanswered, namely, why would the FBI send Sabu targets abroad but only charge the members of LulzSec for violating domestic laws? Additionally, why would none of the latter hackings be used in the formal charge when they are the attacks the FBI has the most information on? The lack of discernible answer leaves me to believe LulzSec was an opportunity for the U.S. Government to launch attacks at key enemies abroad while saving face domestically.

The second category consists of non-state actors that act out of a commitment to ideology or moral imperative. I will refer to members of the 2nd and 3rd compartment as hacktivists for easier

---

[41] Pilkington, Ed. 2013. "Jeremy Hammond: FBI Directed My Attacks on Foreign Government Sites." *The Guardian*, November 15, sec. World news. http://www.theguardian.com/world/2013/nov/15/jeremy-hammond-fbi-directed-attacks-foreign-government.
[42] Ibid.

reference. Hacktivists is a portmanteau of the words hacker and activists and serves to specify how the activists carry out their protest as well as highlight the primarily ideological root of the attack.

These non-state actors are often individuals that feel harmed by a state or private company and seek retribution. The groups typically lack the funds and widespread support to launch a physical insurgency and therefore use the cyber world to send a message. These individuals also tend to be young, anywhere from 13 to 30 years old.[43]

When the second compartment of non-state actors obtain physical weapons, they are often referred to as insurgents or terrorists. In the case of the invasion of American forces in Iraq, as Mary Kaldor explains in her book, New and Old Wars, Iraqi resistance forces were composed of a "loose networks of state and non-state actors, more like a social movement than the typical vertically organized guerrilla insurgency of earlier wars. No one knows the true size of the insurgency."[44] She goes on to summarize that the resistance forces coalesce out of a shared sense of commitment to a cause. Non-state cyber actors function very similarly to real-world actors. The noticeable difference is the greatly increased speed by which cyber actors can organize and coordinate activities in the cyber world. Additionally, non-state cyber actors tend to be physically located in several different states rather than just one location. LulzSec had members located throughout the United States and Europe.

Cyber actors focus more on smaller issues rather than on replacing larger structures. They tend to hyper focus and narrow in on one particular issue and organize around those issues. Once the issue has either been addressed or been found to be unchangeable, the group disseminates.

One of the most famous non-state actors that fall into the second compartment is the hacktivist group Anonymous. Anonymous is a loose, ever-changing, collection of individuals from around the world. Members organize around particular issues and then move onto other issues as they arise. The group is

[43] All the members of LulzSec were under 30 years old.
[44] Kaldor, Mary. 2007. *New and Old Wars: Organized Violence in a Global Era, Second Edition*. 2nd Edition. Stanford, Calif.: Stanford University Press. http://www.amazon.com/New-Old-Wars-Organized-Violence/dp/0804756465/ref=sr_1_3?s=books&ie=UTF8&qid=1398021599&sr=1-3&keywords=mary+kaldor+new+and+old+wars. Pg 158.

responsible for a number of widely publicized attacks. In 2011, Anonymous DDoSed[45] MasterCard, Visa, Paypal, HBGary Federal, and defaced or DDoSed the websites of Tunisia, Egypt, and Libya.[46] The attacks were not significantly damaging, but more of a temporary nuisance to the companies and governments.

Anonymous is also responsible for many high profile attacks against Sony, MasterCard, Visa, the U.S. Department of Defense, the U.S. Department of Justice, the U.S. State Department, the Egyptian government under Hosni Mubarak, the Assad government, the Chinese government, the Israeli government, and various other governmental and non-governmental agencies.[47] Each of the attacks was in protest to a policy or recent action of the government or company. One of the clearest examples of Anonymous' commitment to ideology is their hacking of Israeli websites in retaliation for the treatment of Palestinian people by the Israeli government during Operation Cast Lead. Anonymous took down websites of "government sites like the Prime Minister's office, the Israeli Security Authority, the Immigrant Absorption Ministry, the Defense Ministry and the Israeli Central Bureau of Statistics."[48] The attacks are rarely prolonged and tend to focus on sending a message rather than making significant change to the overall structure. Anonymous' strict commitment to ideology is what keeps them in the second category of non-state actors that act almost entirely out of a commitment to ideology.

In addition to Anonymous, pro-Palestinian hacktivists have launched dozens of attacks against Israeli websites and services.[49] However, attacks are not limited to just government sites. Hacktivists also targeted private industries operating in Israel in order to try and dissuade or discourage the companies'

---

[45] Distributed Denial of Service. A DDoS is akin to thousands of people trying to walk through the same doorway at the exact same time. The result is that virtually all traffic slows to a trickle and effectively renders the website temporarily offline.
[46] Olson, Parmy. 2013. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Reprint edition. New York: Back Bay Books.
[47] Boone, Syrian Electronic Army revealed: Anonymous hacks SEA website; dumps data.
[48] Shehadeh, Lana. 2013. "'Anonymous' Launches New Cyberattacks on Israel - Al-Monitor: The Pulse of the Middle East". News. *Al-Monitor*. April 8. http://www.al-monitor.com/pulseen/originals/2013/04/anonymous-hack-operation-israel-hacktivists-palestine.html.
[49] Carr, Jeffrey. 2010. *Cyber Warfare*. 2nd Edition. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Inc. Pg 22.

involvement in Israel. One estimate puts the number of defacements above 10,000 Israeli sites in 2009.[50]

Prominent cyber security expert, Jeffrey Carr, whose book *Inside Cyber Warfare* is often described as the premier cyber security textbook for military personnel, details some noteworthy groups hacking Israel out of a commitment to pro-Palestinian ideology including Team Evil, Team Hell, Jurm Team, C-H Team, Hackers Pal, Gaza Hacker Team, DNS Team, !TeAm RaBaT-SaLe!, DZ Team, Ashianeh Security Group, and Nimr al-Iraq.[51] I have classified these hacktivists in both the second and third compartments because Palestine is not a full-member state in the United Nations. Therefore, the motivations of those that act on behalf of a Palestinian state are obfuscated by the fact that they could either be working towards the ascertainment of statehood or working towards pro-Palestinian human rights within the state of Israel. My interpretation is that the pro-Palestinian cyber actors are working towards both goals at various points in their existence, thus the dual classification.

Non-state actors that do not have the physical means to launch a protest find cyber means in order to send a message to their supposed aggressor. As technical skills increases I predict that it will be common to see non-state actors join forces on the cyber world more frequently in order to send a message to either a state or non-state aggressor.

We are already starting to see the average citizen join in more cyber attacks as the cost of entry continues to drop and average technical skill increases. The United States has taken extensive efforts to try and quell any form of cyber protests. For example, in 2013, Eric J. Rosol assisted in a DDoS attack against the Koch Industries as part of OpWisconsin, a coordinated effort to take down the Koch Industries website.[52] Rosol is not a technically skilled man and was merely running an automated program he had downloaded online. He was not the orchestrator of the attack nor was he one of its major

[50] Carr, Jeffrey. 2010. *Cyber Warfare*. 2nd Edition. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Inc. Pg 19.
[51] Ibid. Pg 22 – 26.
[52] Coleman, Gabriella. 2014. "The Latest Snowden Revelation Is Dangerous for Anonymous — And for All of Us." *Wired*. February 4. http://www.wired.com/2014/02/comes-around-goes-around-latest-snowden-revelation-isnt-just-dangerous-anonymous-us/.

proponents Rosol was singled out among the attackers and fined $183,000 for damages totaling just $5,000 in order to send a message.[53]

The last compartment of non-state actors are those not organized by the state but nonetheless launch attacks in conjunction with the state out of a sense of nationalism or commitment to state ideology. These hacktivists are different from the second compartment because the attacks are timed to coincide with and reinforce state efforts.

One group with multiple facets is Hidden Lynx. Hidden Lynx is a Chinese hacker group that conducts sophisticated cyber espionage attacks against public and private facilities worldwide. Some of the targets include Google and Adobe along with health care companies, defense contractors, and government agencies.[54] Because of the category of victims, it is difficult to imagine a scenario in which Hidden Lynx is not either A) receiving support from the Chinese government B) being passively allowed to exist or C) somehow being rewarded by the government for at least a portion of their services. Seeing as how filtered the Chinese firewall is, it is ludicrous for the Chinese to pretend they have not noticed the extensive attacks that are routinely launched within its borders. The PLA is trying to advance its economic standing and the actions of Hidden Lynx help improve that standing.

A report released in 2013 by security firm, Symantec, profiled Hidden Lynx as "hired guns working for clients seeking out very specific pieces of data."[55] Hidden Lynx seeks out information that could be then used to benefit the Chinese state. Hidden Lynx differentiates itself from the typical mercenary because they operate only for the betterment of one state, implying some level of tacit approval of state activities. Because Hidden Lynx does not operate for the betterment of multiple states, I have classified them within the third compartment.

---

[53] Matthews, Lee. 2013. "Man Fined $183,000 for Helping Anonymous DDoS a Site for One Minute | Apps and Software | Geek.com". Geek. http://www.geek.com/apps/man-fined-183000-for-helping-anonymous-ddos-a-site-for-one-minute-1579317/.
[54] Finkle, Jim. 2013. "Hacker Group in China Linked to Big Cyber Attacks: Symantec." *Reuters*, September 17. http://www.reuters.com/article/2013/09/17/us-cyberattacks-china-idUSBRE98G0M720130917.
[55] Ibid.

Furthermore, Chinese citizens have shown repeatedly that they will support China using whatever means available. The first instance of Chinese hackers working together for nationalistic interests occurred in 1998. Chinese hackers from all over the country organized a collective response to anti-Chinese protests in Indonesia. Thousands of hacktivists launched coordinated attacks against Indonesian websites, defacing and DDoSing hundreds of websites. Since 1998, the Chinese hackers have only grown stronger, forming guilds and re-emerging every few years to launch coordinated responses. Coordinated attacks of this caliber are characteristic of a cyber skirmish because they escalate beyond the power of a single cyber attack yet they are not quite at the level of a full-scale cyber war.

China also shrouds state activity behind non-state actors. In 2011, Chinese hackers sent an email to G20 delegates advertising "free nude pictures of Carla Bruni...who in 2008 married then French President Nicolas Sarkozy."[56] When recipients clicked the link, the victims unsuspectingly installed a trojan horse that was then used to monitor the communications of the European leaders, reporting the information back to Chinese servers. Though the attacks were never publicly claimed by either a state or non-state entity, there is strong motive and evidence that the Chinese state was behind the attacks. Yet, without such proof the next most likely source is a non-state actor working towards the same end-goal as the Chinese state.

During the 2013 G20 summit, Chinese hackers again performed a phishing attack against European leaders. The attack was traced back to Chinese actors, who could then use the exploited machines to monitor the European representatives. It is again suspected that the attack had government support, but the People's Liberation Army has yet to admit participation.

The second arm of Russia's cyber power is its close connection to shady non-state actors that work in conjunction with state efforts. These non-state actors allow Russia to work in conjunction with former KGB members and the mafia in order to appear innocent while still gaining the benefit of an attack.

---

[56] Finkle, Jim. 2013. "Chinese Hackers Spied on Europeans before G20 Meeting: Researcher." *Reuters*, December 9. http://www.reuters.com/article/2013/12/09/us-china-hacking-g-idUSBRE9B817C20131209.

Russia is responsible for what is widely considered Web War I. In 2007, as a result of long-rising cultural and political tensions, Russia moved troops into Estonia. As part of the attack, Russian hackers flooded the bandwidth of Estonia by flooding the Internet with a massive prolonged DDoS attack.[57] Estonia is heavily reliant on the Internet for its banking needs; in total, "99.6% of banking transactions are done electronically."[58] The DDoS shut down virtually all banking activity. This is the first time Russia used a cyber attack to induce a virtual fog-of-war, which it has done twice since the attack on Estonia.

The Russian government attributed the cyber attacks to patriotic citizens and then took sluggishly slow steps to track down the source of the attack, ultimately finding nothing after an internal investigation. Writing about the rise of a cyber age and non-state actors working in conjunction with states, Dr. Chris Demchak and Dr. Peter Dombrowski explain their role in the 2007 events saying, "As shown by the denial of government and banking service in Estonia in 2007, wholesale assaults across physical borders can be deployed from one state to another by "patriotic hackers," while the originating state claims ignorance and inability to stop the assault."[59] By passing off blame to non-state actors, Russia is able to pass off International outcry into the waiting laps of invisible, non-identifiable actors.

A year later, a major attack originating in Russia was launched against Georgia. Grey Goose, an investigation attempt led by Jeffrey Carr to look into the Russian cyber attack against Georgia, resulted in an absence of solid evidence that the Russian government was working with non-state actors. The report stated, "We assess with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively

---

[57] Brenner, Joel. 2011. *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press. Pg 63.
[58] "Facts about E-Estonia." 2013. *Estonian Information System's Authority*. November 4. http://www.ria.ee/facts-about-e-estonia/.
[59] Rise of a Cybered Westphalian Age. *Chris C. Demchak Peter Dombrowski*. Referencing J. B. Michael et al., "Integrating Legal and Policy Factors in Cyberpreparedness," *Computer* 43, no. 4 (2010): 90–92.

supporting and enjoying the benefits of their actions."[60] The authors strongly suggested that there is a connection, but admitted they could not prove such a connection firmly existed.

In the case of Russia's invasion of Estonia, if the attacks did actually come from a non-state actor, then that group would fall into this third compartment. As of currently, the evidence points to an organization like the Russian Business Network (RBN), a formerly massive server host in St. Petersburg that earned hundreds of millions of dollars hosting the most vile content such as child pornography and murder-for-hires. The RBN would also sell DDoS services at a cost per hour using its massive server farm. It is unclear as of the time of this writing whether or not this was the exact service used and whether for not they were paid by the government. Of notable coincidence, the RBN went almost completely offline soon after the Estonia attacks.[61]

More recently, a group of hacktivists calling themselves the "cyber berkut" temporarily took down sites of NATO forces in March 2014.[62] Jeffrey Carr explains the cyber berkut are a pro-Russian hacker collective that are responding to NATO pressure to join the E.U.[63] The attack used a basic DDoS attack to temporarily limit access to the sites. The attack against NATO is just a series of attacks used by cyber berkut to advance pro-Russian support.

When looking at the future of cyber warfare we should expect to see the rise of average citizens launching cyber attacks. The attacks will not necessarily be damaging, but the ease of which they can be launched and the high commitment to ideological components in the cyber world will create the necessary environment for more cyber attacks. These conditions are especially true in non-developed countries

---

[60] Clarke, Richard A., and Robert Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It*. Reprint edition. New York: Ecco. Pg 115.
[61] Warren, Peter. 2007. "Hunt for Russia's Web Criminals." *The Guardian*, November 14, sec. Technology. http://www.theguardian.com/technology/2007/nov/15/news.crime.
[62] Croft, Adrian, and Peter Apps. 2014. "NATO Websites Hit in Cyber Attack over Crimea Stance." *Chicago Tribune*. March 15. http://articles.chicagotribune.com/2014-03-15/business/sns-rt-us-ukraine-nato-20140315_1_cyber-attacks-nato-interference-u-s-cyber-consequences.
[63] Carr, Jeffrey. 2014. "Digital Dao: Cyber Berkut and Anonymous Ukraine: Co-Opted Hacktivists and Accidental Comedians." *Digital Dao*. http://jeffreycarr.blogspot.com/2014/03/cyber-berkut-and-anonymous-ukraine-co.html.

where the lack of monitoring infrastructure allows serious hackers and hacktivists to hide his or her activities more easily without the fear of punishment.

These attacks will see significant jumps when done in retaliation to a perceived threat or attack. For example, if Iran or North Korea were to attack California's power infrastructure with a major cyber attack, then the wealth of coders that would be affected by the attack could result in homegrown cyber attacks. Similarly, if an attack turns into full-scale war then citizens that do not want or physically cannot join the army will be able to find a unifying and inspiring environment by working with other non-state actors to launch attacks.

Some states can never have a civilian cyber population under the current system. Jeffrey Carr explains, "North Korea doesn't have the infrastructure to sustain a civilian hacker population. All of its money and all of its talent (meaning young people who show the requisite abilities) are part of its military establishment."[64] Thus, if an attack stems from North Korea it is almost guaranteed to be the workings of the state.

State and non-state cyber actors will continue to grow in technical capabilities and frequency of attacks. Understanding the underlying motivation and technical capabilities can help both identify the origin of an attack as well as predict the effectiveness of the attack. In the cyber world, the offense is heavily advantaged because of the wealth of targets available and the relatively low threshold for defenses structures. In the next chapter, I will discuss the strategy used by attackers and discuss the two main types of vulnerabilities used by hackers.

[64] Carr, Jeffrey. 2010. *Cyber Warfare*. 2nd Edition. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Inc. Pg 82.

CHAPTER 3: OFFENSIVE CYBER STRATEGY

"Given enough time, motivation and funding, a determined adversary will always – always be able to penetrate a targeted system."[65] - Steven Chabinsky, FBI.

Cyberspace was not designed with security in mind. The original users were researchers and university professors that used the Internet to communicate rapidly with each other. They did not foresee that the Internet could become any larger than their small group. As more users came online it soon became apparent how cyberspace was designed with a complete lack of inherent defenses.

In this chapter I will discuss overall cyber strategy and explore a number of key questions regarding the future of U.S. activities in cyberspace including: What vulnerabilities should we expect to see in the future? How does the United States protect itself in the cyber world? How do other states protect themselves? These are some of the questions I will address in this chapter.

In cyber warfare, the balance is heavily weighted towards an offensive strategy. The multiplicity of available targets makes the job of defending every single point of vulnerability almost unimaginable. Dr. Ilai Saltzman, assistant professor at Claremont McKenna College, explains the ramifications of a cyber attack against a state target saying:

> Strategic targets or critical infrastructures consist of vital or centre-of-gravity assets whose destruction may have a colossal effect on a state's national security and its capacity to operate normally. Such elements include a state's military constellations, defence industrial base, satellite communication, electrical power grid, internet connectivity, central banking system, stock market, ministries, and governmental agencies.[66]

Targeting any of these vulnerabilities can result in the catastrophic paralyzation of society. Current cyber defensive strategies are extensions of physical defense strategies and thereby mandate that all points of critical vulnerability be protected. However, as Chabinsky points out, a determined attacker will always be able to penetrate the target system.

---

[65] "War In The Fifth Domain." 2010. *The Economist*, July 1. http://www.economist.com/node/16478792.
[66] Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy*, March. http://dx.doi.org/10.1080/13523260.2013.771031. Pg 43 - 44.

Vulnerabilities exist on either a vertical or horizontal plane. Understanding each type of vulnerability is critical to understanding why states and non-states in particular favor cyber offensive strategies. Vertical vulnerabilities are primarily those that exist in the software hierarchy level. For example, the following chart shows the hierarchy of software running on a sample computer:

Hardware Software: BIOS
Operating System: Microsoft Windows 7
Programs: Oracle Java, Microsoft Office, iTunes, Chrome, Firefox,
Vulnerability: Reflection API located within Java program

In the above case, the vulnerability is buried within a small segment of code located within a single program, Java. The above exploit is a real exploit that resurfaced in 2013 after a security update from Java ironically enabled a 10-year old moot attack useful.[67] The vulnerability allows "the remote execution of code outside the Java sandbox."[68] In this case, the initial exploitation opens up the larger system (operating system, programs, and BIOS) to a vast array of further points of vulnerability. Vertical vulnerabilities are dependent upon the technical makeup of the system.

In contrast to vertical vulnerabilities, horizontal vulnerabilities exist laterally across systems and are usually due to human error, such as using the same password for multiple accounts. In 2010 Aaron Barr, CEO of HBGary Federal, announced he could gather data on the famous Anonymous network via social engineering (a type of horizontal vulnerability). In retaliation to his claims, he then became the subject of one of the most widely popularized campaigns launched by members of Anonymous. After exploiting a vertical vulnerability found within the MySQL database software on the HBGary website, members of Anonymous were able to crack one of Barr's passwords, "kibafo33" that Barr also used to sign into the company's website. The hacktivists then tested the same password on his "Twitter, Yahoo!, Flickr, Facebook, and even World of Warcraft"[69] account. Barr had used the same password for all of his

[67] Constantin, Lucian. 2013. "New Vulnerability in Java 7 Opens Door to 10-Year-Old Attack, Researchers Say." *PCWorld*. July 18. http://www.pcworld.com/article/2044670/new-vulnerability-found-in-java-7-opens-door-to-10yearold-attack-researchers-say.html.
[68] Mimoso, Michael. 2013. "Old Attack Exploits New Java Reflection API Flaw." *Threat Post*. July 18. http://threatpost.com/old-attack-exploits-new-java-reflection-api-flaw/101388.
[69] Olson, Parmy. 2013. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Reprint edition. New York: Back Bay Books.

accounts. One vertical vulnerability now exposed Barr horizontally across multiple different platforms, leaving Barr open to one of the most embarrassing attacks launched against a security company. After planning the attack for a few days, the hacktivists opened fire all at once leaving Barr unable to react or protect himself. The hacktivists published all of Barr's research, eliminating the possibility of him selling the information to the federal government. After eliminating his profit material, the hacktivists published his social security number, home address, phone number, online account name, and all of his emails online.

Repeating the same password is a very common practice that creates overall less secure systems. This is especially true if the password is repeated between public and private systems, as in the case of Aaron Barr's "kibaffo33." Additionally, many people use a repeatable pattern to create passwords such as "a root plus an appendage."[70] Breaking one password can lead to solving many others if the same system is repeated.

Major attacks orchestrated by the state tend to favor vertical vulnerabilities because of the technical resources available as in the case of Stuxnet, Duqu, Flame, QUANTUMBOT, and TURBINE. Non-state actors tend to favor a combination of vertical and horizontal vulnerabilities because they require less technical skills and more interpersonal skills. As demonstrated in the HBGary case, a small vertical vulnerability opened up massive horizontal capabilities.

In April 7, 2014 the now famous heartbleed vulnerability was made known to the public through a series of reports started by the Finnish cyberscurity company, Codenomicon.[71] Heartbleed is a result of a single typo in the encryption mechanism that then allowed for hackers to retrieve account information (along with a lot of other information) of other users. The exploit is a prime example of vertical

---

[70] Schneier, Bruce. 2014. "Choosing Secure Passwords." *Schneier on Security*. https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.
[71] http://heartbleed.com/

vulnerabilities waiting in the wild to be seized. Many in the security field, including Bruce Schneier, have referred to heartbleed as one of the most catastrophic events for Internet security.[72]

The rapidity with which non-state actors can operate in the cyber world gives them a strategic advantage for out maneuvering their opponents. The members of non-states do not have to report to command centers or abide by international law when planning an attack. Team Hell, Team Evil, the Syrian Electronic Army, and the multiplicity of non-states actors are free to coordinate amongst themselves in order to organize and execute attacks. Additionally, the relative anonymity of non-state actors gives them a strategic out if they ever find themselves too deep. Yet, now that many governments are heavily active in cyberspace, the idea of remaining truly anonymous online is quickly becoming a fleeting reality.

As of now, states are largely employing an offensive strategy in that each state has penetrated core systems of other states but has yet to make its presence known. The files leaked by Edward Snowden reveal that the United States has penetrated the networks of several of its close allies. The penetrations served as key points of vulnerabilities incase of emergency. I will speak more on those leaks in chapter 7.

The vulnerabilities only work when the target is unaware that the vulnerabilities exist. As a result of the revelations, the United States will now have to develop and implement new logic bombs for use in case of emergency. States are likely to use both vertical and horizontal vulnerabilities to attack their targets. Given enough financial resources, manipulating a human target in order to create vulnerabilities is easiest for state actors. However, if the state wanted to maintain total secrecy then using vertical vulnerabilities is the preferable method as it inherently isolates the number of personal involved.

Non-states do not typically have to focus on a significantly defensive strategy because they have very little infrastructure to defend. The few laptops, cell phones, tablets, or small servers are easily reproducible if destroyed or taken. Non-states' capital rests not in the physical infrastructure, but rather in the social capital of the population.

---

[72]Schneier, Bruce. 2014. "Heartbleed." *Schneier on Security*. https://www.schneier.com/blog/archives/2014/04/heartbleed.html.

For states or non-states to form an adequate defensive capability, each point of vulnerability must be addressed in order for the system to be secure. To form an excellent defensive capability, vertical vulnerabilities must be isolated from horizontal vulnerabilities. To form a near-perfect defensive capability, resilience must be added to the systems in order to be able to withstand multiple attacks unphased. Defense scholar Peter Singer, a noted proponent of resilient networks as a defensive strategy, explains the concept of resilience in his book saying, "A key to resilience is accepting the inevitability of threats and even limited failures in your defenses. It is about remaining operational with the understanding that attacks and incidents happen on a continuous basis."[73] State networks that wish to be successful in the cyber world must develop resilient networks capable of functioning regardless of the number of ongoing attacks.

There are only a few general defensive strategies for combating vertical vulnerabilities. The most common tactic for Microsoft operating systems is to use anti-virus software like Kaspersky, McAffee (now known as Intel Security), AVG, and a host of other solutions in combination with running routine software updates. Anti-virus software functions by identifying known malware and then scanning the local machine for signatures of the virus (or worm, trojan horse, exploit, rootkit, etc). Developing anti-virus is completely reactionary and dependent on a timely response from the private company to control the spread of the malware. Once the virus signature has been identified, each device owned by the agency must then be scanned to rule out infection. For the United States to effectively rely on anti-virus software then each of the machines privy to high-level government intelligence must all be updated.

The private sector faces the same issues related to creating intrusion-proof systems. In 2013, "the Syrian Electronic Army targeted websites belonging to *CNN*, *Time Magazine* and the *Washington Post* by breaching a third party service used by those sites."[74] The third party was an ad-service that the SEA was

[73] Singer, Peter W.; Friedman, Allan (2013-11-16). Cybersecurity and Cyberwar: What Everyone Needs to Know (p. 36). Oxford University Press, USA. Kindle Edition.
[74] Shih, Gerry, and Joseph Menn. 2013. "New York Times, Twitter Hacked by Syrian Group." *Reuters*, August 28. http://www.reuters.com/article/2013/08/28/net-us-newyorktimes-hacked-idUSBRE97Q11J20130828.

able to gain access to through basic social engineering. Once inside, SEA was able to reroute links to its own private server to try and trick viewers to download its custom-built malware. The SEA attack demonstrates that vulnerabilities can exist in multiple different layers; one vertical vulnerability can open up the system to more extensive exploits.

Binary attempts to define network security mean that if one computer is vulnerable then the entire system is vulnerable. Understanding network security based on a spectrum between secure and insecure allows for a more fitting analysis of cyber security. There can never be a system that is 100% secure, but rather it can be regarded as *mostly* secure according to a spectrum.

While anti-viruses are generally successful for the average individual, the rate at which anti-virus companies can discover, process, and release virus signatures is decreasing, thereby opening up more vulnerabilities for government offices. As of today, there are over 60 million signatures for viruses and that number is rapidly increasing. Speaking at a CSIS Conference in May 21, 2013, David DeWalt, CEO of FireEye, explains the enormity of the threats saying:

> We see 60,000 pieces of malware everyday. The average company is infected 100 times a day. 100 times a day actually infected - successful infections, on average. Every couple of seconds there is an attack...We see 9,000 new websites created everyday that are malicious because of the lack of governance model...We have hundreds of thousands command and control servers set up around the world. 94% of the countries in the world today are active with hosting command and control servers.

Purely reacting to threats is becoming harder to do as the gap between the ability to create and attack and the ability to defend against an attack is widening. Unless changes are made to the defense model, a reactionary strategy will soon become woefully incapable of keeping up with the growing number of exploits. The inevitability of anti-virus companies to keep up with the creation of malware is yet another reason for states to build resilient networks, expecting to be one day exploited with safety plans already in place.

One of the upcoming critical points of failure is Microsoft's famous Windows XP. Windows XP, formerly the most widely used operating system in the world, was released in 2001 with a grand total of 45 million lines of code. From those 45 million lines of code millions of exploits have been discovered and

utilized by hackers. Every time a vulnerability is patched it potentially creates dozens of new vulnerabilities that can be similarly exploited. This number is expounded when we also consider the additional software that individuals and companies utilize in addition to just the operating system.

After over a decade of active support, Microsoft has announced that it will stop releasing free security updates for the operating system in April 2014. Companies and governments will have the option to pay a high fee in order to receive security updates. The ending date has been pushed back several times already in order to both warn system administrators and allow them time to transition to a newer more secure operating system. Despite warnings, much of the world's IT infrastructure still runs on the soon to be extremely vulnerable operating system.

One of the biggest vulnerabilities that has a high potential to be exploited lies in bank ATMs. 95% of the world's ATMs run on a modified version of Windows XP. A single vulnerability found in one ATM would be able to be repeated in hundreds of other ATMs, opening up the potential for significant cyber exploits.

Additionally, many hospitals still run mission critical hardware on Windows XP. In February, 2014, security analysis Robert Austin took his 38-week pregnant wife to have the baby flipped in preparation for delivery. While waiting for the procedure, he noticed a familiar sight on one of the machines and subsequently tweeted a picture of the hospital's medical equipment doing a routine check disk.[75] The check disk utility is used primarily used to fix corrupted operating systems or disks.

Come April 8th, hospitals running Windows XP will no longer be HIPAA compliant.[76] HIPAA, or the Health Insurance Portability and Accountability Act of 1996. HIPAA is used to maintain security for hospitals and protect patients' privacy. In order to remain complaint, hospitals will need to shell out millions of dollars to pay Microsoft to continue releasing security updates to their machines.

---

[75] Austin, Robert. 2014. "@W3nd1g04n6". Twitter. https://twitter.com/W3nd1g04n6/status/437946054613688320.

[76] Hamilton, Alex. 2014. "Thousands of Government PCs Will Expose Themselves to Malware as Windows XP Expires." *TechRadar*. January 14. http://www.techradar.com/news/software/operating-systems/thousands-of-government-pcs-will-expose-themselves-to-malware-as-windows-xp-expires-1215033.

In England, the National Health Service began transitioning off of Windows XP, but has already recognized that the transition will not meet the April 8th deadline.[77] The NHS has instead chosen to pay Microsoft a subscription fee for extended updates while it continues to move its systems to a newer operating system.

Transitioning to a new operating system or software can be cumbersome, time consuming, and most importantly, expensive. In 2009 the Army began looking for a unified email solution to its 440 independently operated networks. In 2011 it selected Microsoft Exchange service (the same one Tufts uses) and the rollout was finally completed at the turn of 2014.[78]

Undoubtedly, part of the difficulty with any branch of the U.S. government rolling out any new IT system is the ability to maintain security and daily operations. Yet, the larger issue is the bureaucratic red tape that latches on and hinders government cyber projects. The U.S. Government is not designed for quick IT solutions. The interplay between Congress, the Department of Defense, private contractors, and the many platoons involved in cyber conflict all contribute to an overall less effective system. The inability of the U.S. government to quickly roll out new projects and solutions will leave it notably defenseless in the cyber world.

On a small scale, the U.S. uses anti-virus software on its many machines to defend itself from general viruses and infections. In 2002, Congress passed the Federal Information Security Management Act (FISMA), which mandates a baseline security standard for each federal agency. Part of following FISMA is maintaining security updates and anti-virus software for all computers.

On a larger, state-to-state or state-to-major-non-state level the U.S. follows a policy of "active defense". Thom Shanker writing for the New York Times explains, "officials say that the United States needs to maintain "active defenses" in cyberspace, a concept that seeks to identify and even neutralize

---

[77] Hamilton, Alex. 2014. "Thousands of Government PCs Will Expose Themselves to Malware as Windows XP Expires." *TechRadar*. January 14. http://www.techradar.com/news/software/operating-systems/thousands-of-government-pcs-will-expose-themselves-to-malware-as-windows-xp-expires-1215033.

[78] Gallagher, Sean. 2013. "Why US Government IT Fails so Hard, so Often." *Ars Technica*. October 10. http://arstechnica.com/information-technology/2013/10/why-us-government-it-fails-so-hard-so-often/.

threats before they hit a Defense Department network."[79] The Department of Homeland Security is responsible for maintaining the civilian cyber defense capabilities. Yet, there is yet to be a clear delineation for when the DHS should get involved in a cyber conflict.

The larger active defense strategy mirrors the preemptive strike strategy used by the Bush Administration to justify going into Afghanistan and then Iraq.[80] Both involve identifying possible major attacks against the United States and then eliminating the threat before it has time to reach fruition. That is not to say the United States is neglecting its defensive capabilities, simply that the United States takes on a more active elimination approach.

Once a state or non-state has been identified as intending to launch a cyber attack against the United States, "The Pentagon has made it clear it would employ force to defend against cyber attacks."[81] A pre-emptive strike can be physical or cyber. Farwell and Rohozinski later point out that there is still confusion regarding who has the final authority to assess when an impending force is going to be used. They draw attention to the lack of formal policies that translate laws that govern the physical world into the cyber world.[82] Can a battleship actively pursue hackers it believes were planning to launch an attack against the ship?

The laws surrounding active defense are still ambiguous because international policy and precedent has yet to be solidified for the various stages of cyber conflict. In 2011, the United States debated using a cyber attack to neutralize Libya's air defense system before an air raid. The attack was eventually called off because top U.S. officials feared that "it might set a precedent for other nations, in

---

[79] Shanker, Thom. 2011. "U.S. Weighs Cyberwarfare Strategy." *The New York Times*, October 18, sec. World / Africa. http://www.nytimes.com/2011/10/19/world/africa/united-states-weighs-cyberwarfare-strategy.html.
[80] Dinan, Stephen. 2008. "Bush Defends Pre-Emptive Strike Doctrine." *The Washington Times*. December 9. http://www.washingtontimes.com/news/2008/dec/9/bush-defends-pre-emptive-strike-doctrine/.
[81] Frawell, James, and Rafal Rohozinski. 2012. "The New Reality of Cyber War." *Survival: Global Politics and Strategy* 54 (4): 107–20. doi:10.1080/00396338.2012.709391. Pg 110.
[82] Ibid.

particular Russia or China, to carry out such offensives of their own".[83]

Despite the decision to not launch a preemptive cyber strike in Libya, there has already been a developing precedent for a preemptive cyber strike before military involvement. In the previous chapter, the example of Israel launching an air strike on Syria in 2007 involved use of a preemptive cyber strike. Before the United States invaded Iraq, U.S. cyber forces hacked the Iraqi Intranet used by troops to communicate with each other. The U.S. sent a single email to all Iraqi soldiers warning of the impending attack and instructing the soldiers to leave their military vehicles outside of the base to be destroyed via an impending air strike. When Russia invaded Estonia in 2007 Russian non-state actors flooded the Estonian network with bogus traffic in order to induce a virtual fog of war. A preemptive cyber attack has shown to be a surefire way to reduce oppositional forces before engaging in a physical attack.

Other states do not follow the same active defense model followed by the United States. On the other end up the spectrum, China has created a more fortress-like approach. China, in both its massive populous and fortified networks has designed itself to be able to withstand an onslaught of physical and cyber assaults.

China's cyber infrastructure is composed of two major cyber infrastructures. The first piece funnels all Internet traffic through a government run firewall called the Golden Shield Project. Since its implementation in 2003, the firewall weeds out subversive web content and acts as a first-layer of defenses against possible intrusions. The firewall works by operating on all Internet gateways in and out of China and scanning all traffic in real time. There are three major gateways that China has to monitor located in Shanghai, Taipei, and Hong Kong.[84] China can use this firewall to also sever all communication ties leading in and out of the country. In case of a major attack China could completely isolate itself from the rest of the world.

---

[83] Schmitt, Eric, and Thom Shanker. 2011. "U.S. Debated Cyberwarfare Against Libya." *The New York Times*, October 17, sec. World / Africa. http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

[84] "The Internet's Undersea World". Digital Map. http://ansonalex.com/wp-content/uploads/2011/02/underwater-internet-cable-map.jpg.

The second major design is the compartmentalization of infrastructure. If China believes itself to be under a major cyber threat then it cannot only isolate itself from the rest of the Internet, it can also compartmentalize its Internet-connected infrastructure to become more secure. In order for an attack against Chinese infrastructure to be successful it would need to A) originate in China in order to get passed the firewall B) target specific infrastructure within the isolated pocket.

The policy of active defense has a limited impact against non-state actors because of the differences in organization. Non-state actors tend to have a high level of mobility as compared to state actors. In the physical world, non-state actors can organize in coffee houses, public parks, schools, libraries, etc. Most commonly, non-state actors meet in cyber chat rooms and private web forums for easier communication and organization. Using a policy of active defense in order to eliminate the non-state actors' chartroom or web forum is virtually meaningless because a new website can be setup and publicized within a few hours. The effect is a virtual cat and mouse as state actors chase non-state actors through the depths of cyber space.

The best strategy against non-state actors is also the most time consuming - physically tracking the cyber actors. In the case of LulzSec, the cyber ring was eventually taken down because agents from several different countries cooperated in order to arrest the hackers. Similarly, Cold Zero, a member of Team H3ll, "was caught in a 'honey pot' set up by authorities" in Israel.[85] There is no better way to eliminate a cyber threat than physically capture the cyber actors. Alternative attempts to discredit the legitimacy of an attacker prove fruitless because the cyber actor can create a new identity with a new name in a matter of moments.

The United States' capabilities as a major cyber actor did not come cheap or easy. Major investments by Congress and the DoD have heavily shaped the United States' cyber capabilities. In the next chapter, I will follow the money and personnel exchange between the public and private sector in an effort to shed more light on the United States' cyber operations.

---

[85] Carr, Jeffrey. 2010. *Cyber Warfare*. 2nd Edition. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Inc. Pg 23.

CHAPTER 4: THE CREATION OF A MILITARY DIGITAL COMPLEX

On January 17, 1961, former President Dwight D. Eisenhower departed the office of the Presidency in his farewell address. Before he left, he warned of the growing influence of the Military Industrial Complex (MIC), an iron triangle between the government agencies, the military, and the private industry to fuel the perpetuation of war.

With the advent of cyber weapons, the old concept of the military industrial complex has evolved to envelop the creation and implementation of cyber weapons and defensive cyber infrastructure. The evolution of the MIC to a slightly different entity is called the Military Digital Complex (MDC), which is the focus on this chapter.[86] I will first speak generally on the cost of cyber weapons as compared to other weapons. I will then discuss the use of private contractors for cyber operations and the rise of cyber contracts. I will finish by discussing the close ties that exist between private and public industry.

The United States' defense spending is undoubtedly the highest in the world. In 2012, the United States spent $645.7 billion on defense and that does not include the additional funds for maintaining its nuclear arsenal.[87] $645.7 billion dwarfs the next closest nation, Russia, which reportedly only spends $126 billion on defense.[88] The DoD, responding to pressure from Congress, is seeking to reduce total spending while simultaneously invest more in cyber capabilities. In the Fiscal Year 2013 Budget Request, the opening paragraph explains, "The Fiscal Year (FY) 2013 President's Budget develops a defense strategy to transition from emphasis on today's wars to preparing for future challenges…and supports the national

[86] Some scholars call the complex the Cyber Industrial Complex. For the purpose of consistency I will use the term Military Digital Complex.
[87] "United States Department of Defense Fiscal Year 2013 Budget Request." 2014. Budget Request 4-0609CA0. Washington, D.C.: The Department of Defense. http://dcmo.defense.gov/publications/documents/FY2013_Budget_Request_Overview_Book.pdf. Pg 1-1
[88] "Defense Spending By Country." 2014. *Global Fire Power*. http://www.globalfirepower.com/defense-spending-budget.asp.

security imperative of deficit reduction through reduced defense spending."[89] Preparing for future challenges is a euphemism for developing advanced cyber capabilities, among other weapon types.

Cyber weapons include only the operations that are launched in cyberspace. To maintain a common definition of cyber operations and cyber spending, I will not include the infrastructure costs or the server costs to house the data needed to launch any sort of cyber attack. The cost of collecting data that then leads to an attack adds an additional $20 billion to the total.[90] In 2013, the Pentagon released its new cyber budget predicting to spend $23 billion through 2018.[91]

In 2012, the Pentagon requested $2.3 billion in its budget proposal for cyber spending.[92] For 2014, the pentagon has requested $5.1 billion for cyber spending.[93] Peter Singer explains the increased focus on cyber spending saying:

> Indeed, the Pentagon's 2013 budget plan mentioned "cyber" 53 times. Just a year later, the 2014 budget plan discussed "cyber" 147 times, with spending on CYBERCOM's headquarters alone set to effectively double (all the more notable as the rest of the US military budget was being cut).[94]

Besides the official request, the black budget released by the *Washington Post* adds an additional $4.3 billion to cover cyber operations conducted by the Central Intelligence Agency, National Intelligence Agency, the National Reconnaissance Office, and the National Geospatial Intelligence Program.[95] The $4.3 billion includes only the cost of the operation and does not factor in the equipment costs. Though a few billion

---

[89] "United States Department of Defense Fiscal Year 2013 Budget Request." 2014. Budget Request 4-0609CA0. Washington, D.C.: The Department of Defense. http://dcmo.defense.gov/publications/documents/FY2013_Budget_Request_Overview_Book.pdf. Pg 1-1

[90] Andrews, Wilson, and Todd Lindeman. 2013. "The Black Budget." *The Washington Post*, August 29. http://www.washingtonpost.com/wp-srv/special/national/black-budget/.

[91] Capaccio, Tony. 2013. "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion." *Bloomberg*, June 10. http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html.

[92] "DoD Cybersecurity Spending: Where's the Beef?" 2011. Defense Program Analysis. *Defense Industry Daily*. http://www.defenseindustrydaily.com/cyber-security-department-defense-spending-06882/#money.

[93] Capaccio, Tony. 2013. "Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion." *Bloomberg*, June 10. http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html.

[94] Singer, Peter W.; Friedman, Allan (2013-11-16). Cybersecurity and Cyberwar: What Everyone Needs to Know (p. 134). Oxford University Press, USA. Kindle Edition.

[95] Andrews, Wilson, and Todd Lindeman. 2013. "The Black Budget." *The Washington Post*, August 29. http://www.washingtonpost.com/wp-srv/special/national/black-budget/.

dollars could easily match the spending several small nations, compared to the overall defense the requested funds are noticeably low because cyber operations are generally cheaper than other methods of warfare.

For comparison, the Global Hawk UAV cost $211 million per drone for a total cost of $13.9 billion.[96] That is the cost of just one group of UAVs and does not include the cost of running the program or supporting systems. The additional costs amount to at least an additional $6.6 billion.[97] For further comparison, the F-35 Lightning II aircraft, rated as a fifth-generation fighter, is expected to cost a staggering $1 trillion when factoring in initial price tag and operating costs.[98] [99] As compared to drone strikes and next-generation aircrafts, cyber attacks are significantly cheaper to develop, maintain, and carry out. Thus, as the DoD works to reduce spending in old forms of warfare, transferring just a portion of the funds towards cyber research helps to develop advanced 21st weaponry while also reducing costs.

The $5.1 billion (not counting the unofficial $4.3 billion) requested for cyber spending is also artificially low because of the widespread use of contractors to research and develop cyber weapons. Contractors make up a significant portion of spending and capabilities for U.S. weapons development.

The DoD spends $75 billion yearly on private contractors for U.S. intelligence operations.[100] Private contractors include groups such as Booz Allen Hamilton, Academi, Northrop Grumman, General Dynamics, Science Applications International Corp (SAIC), Data Tactics Corp, Raytheon SI Government Solutions, and the hundreds of other defense contractors through which the federal government operates. Not all of the spending goes towards cyber operations, but the DoD's push for more

---

[96] Gertler, Jeremiah. 2012. "U.S. Unmanned Aerial Systems". CRS Report for Congress 5-5700. Congressional Research Service. http://www.fas.org/sgp/crs/natsec/R42136.pdf.
[97] Roberts, Amy. 2014. "By The Numbers: Drones." *CNN*. Accessed April 21. http://www.cnn.com/2013/04/05/politics/drones-btn/index.html.
[98] Tierney, Dominic. 2011. "The F-35: A Weapon That Costs More Than Australia." *The Atlantic*. March 15. http://www.theatlantic.com/national/archive/2011/03/the-f-35-a-weapon-that-costs-more-than-australia/72454/.
[99] Dillow, Clay. 2014. "Budget Deal a Win for Defense Contractors - Fortune Tech". News. *CNNMoney*. http://tech.fortune.cnn.com/2014/01/17/budget-deal-a-win-for-defense-contractors/.
[100] Dilanian, Ken. 2010. "Intelligence Nominee's Contractor Ties Draw Scrutiny." *Los Angeles Times*, July 25. http://articles.latimes.com/2010/jul/25/nation/la-na-clapper-contractors-20100725.

focus on cyber indicates that a growing percentage of those funds will undoubtedly be put towards cyber related activities.

Besides the DoD's spending, individual states are developing cyber capabilities in order to better police the Internet. California just created a new California Cybersecurity Task Force in 2013 with the responsibility of working with public and private agencies to develop a more secure cyberspace.[101] The FBI contributes over $86 million towards the cyber industry through its Next generation Cyber initiative.[102] In total, the cyber industry is estimated to be worth around $65 billion and could be worth as much as $165 billion in 10 years when including private and public investments.

Beyond the exchange of money, the exchange of personnel is critical to the growth and maintenance of the MDC. The MDC funnels personnel and money between government agencies, military, and defense contractors. According to a report by the Washington Post, "thirty percent of those with top-secret clearances are contractors."[103] Contractors are useful for the federal government because they have less regulation and oversight as compared to federal agencies. Defense contractor employees with top-secret security clearances are allowed to work on a wider array of contracts, thereby opening up the total available contracts for which the company can compete.

Defense contractors create a wide range of military equipment including fighter jets, ships, guns, radar equipment, etc. In the past five years, defense contractors have transitioned their efforts away from expensive physical equipment and begun focusing more on the development of cyber weapons and cyber defenses.

Defense contractors are attracted to the field of cyber operations because of the high profit margins and the move away from more expensive physical parts to cheaper cyber contracts. In its Annual Report, BAE Systems publishes their data on each of their five programs. In 2012, BAE Systems reported

---

[101] Wood, Colin. 2013. "California Launches Cybersecurity Task Force." *Government Technology*, May 17. http://www.govtech.com/security/California-Launches-Cybersecurity-Task-Force.html.
[102] "Fiscal Year 2014 Authorization and Budget Request to Congress." 2013. U.S. Department of Justice Federal Bureau of Investigation. http://www.justice.gov/jmd/2014justification/pdf/fbi-justification.pdf.
[103] Dilanian, Ken. 2010. "Intelligence Nominee's Contractor Ties Draw Scrutiny." *Los Angeles Times*, July 25. http://articles.latimes.com/2010/jul/25/nation/la-na-clapper-contractors-20100725.

an 8.8% return on sales in its Cyber & Intelligence activities.[104] Additionally, cyber operations require advanced equipment in order to function. The return on sale for the cyber equipment yields a significantly higher 14.3%.[105]

Northrop Grumman, the third most profitable defense contractor, reports a total sales of $28 billion in 2012, over $17 billion of that coming from electronic systems, information systems, and technical services - all related in some form or another to the development of cyber weapons, cyber defenses, and cyber services.[106] Not all of that $17 billion is drawn directly from the DoD budget. Northrop Grumman also contracts with the FBI and DHS among other agencies. Northrop Grumman states cyber security as one of its key focus areas for development.[107]

Examining the accounts of virtually any defense contractor reveals increasingly more frequent contracts associated with cyber operations from all branches of the military. On May 31, 2013, Data Tactics Corp was awarded a $25,796,741 cost-plus-fixed-fee contract by the Air Force in order to build a new way to collect, graph, and analyze network data.[108] On the same day, Raytheon SI Government Solutions was similarly awarded a $9,752,133 cost-plus-fixed-fee contract by the Air Force for "Plan X mission execution software."[109] Raytheon SI Government Solutions will "develop a runtime environment to both securely and efficiently execute cyber operations mission scripts and to serve as a foundation for cyber support platforms."[110] Ten years ago there would rarely have been one cyber contract. The presence of two contracts in one day indicates a growing presence of cyber contracts. The number of cyber contracts is quickly growing as the DoD, at the behest of the President Obama, invests more funds into all forms of cyber operations.

---

[104] "BAE Systems Annual Report 2012". BAE Systems. http://bae-systems-investor-relations-v2.production.investis.com/~/media/Files/B/BAE-Systems-Investor-Relations-V2/Annual%20Reports/BAE-annual-report-final.pdf.
[105] Ibid.
[106] "Northrop Grumman Annual Report 2012." 2013. Annual Report. http://www.northropgrumman.com/AboutUs/AnnualReports/Documents/pdfs/2012_noc_ar.pdf.
[107] Ibid. Pg 3.
[108] "U.S. Department of Defense Contracts." 2013. 384-13. U.S. Department of Defense. http://www.defense.gov/contracts/contract.aspx?contractid=5053.
[109] Ibid.
[110] Ibid.

On September 21, 2012 the Navy awarded a contract to Booz Allen Hamilton "not to exceed $9,917,282 firm-fixed-price, indefinite-delivery/indefinite-quantity contract"[111] for helping to prepare the Operational Designated Approval Authority and the Office of Compliance and Assessment for systems accreditation. Specifically, "assisting the OCA with conducting command cyber readiness inspections and cyber security inspections."[112]

On January 8, 2010 Lockheed Martin was awarded an $8,121,044 cost-plus-fixed-fee contract by the Army in order to build a "working prototype that demonstrates the capabilities of the National Cyber Range."[113] The contract explains "the NCR will enable a revolution in the nation's ability to conduct cyber operations by providing a persistent cyber range."[114] In all branches of the military, money devoted for cyber operations is increasing whereas spending for more expensive weaponry is decreasing to reflect the economic downsizing of the DoD.

The DoD has been pushing for more competitively awarded contracts, as they allow for more transparency in the bidding process. The Navy contract awarded to Booz Allen Hamilton was not competitively procured. There is a long-standing stigma against non-competitive contracts as they could be signs of cronyism. In 2011 the DoD aimed for 65% of contracts to be competitively awarded and fell just short of that goal at 58.5% of contracts competitively awarded.[115]

Post 9/11, private contractors were seen as an easy and efficient method to gain additional employees without having to go through the notoriously slow hiring process for federal employees. However, it soon became apparent that contractors could offer substantially more funds to employees, which then drove up the costs of employees as companies competed over limited technical employees. As contractor salaries rose, more federal employees operating in cyber space transferred to the private sector to do the same job for a higher salary.

---

[111] "U.S. Department of Defense Contracts." 2012. 384-13. U.S. Department of Defense. http://www.defense.gov/contracts/contract.aspx?contractid=4882.
[112] Ibid.
[113] "U.S. Department of Defense Contracts." 2010. 384-13. U.S. Department of Defense. http://www.defense.gov/contracts/contract.aspx?contractid=4198.
[114] Ibid.
[115] FY 2013 Defense Budget. 7 – 25.

The use of private contractors has exploded so fast that keeping track of how many are active has proven to be a challenge within itself. While serving as Secretary of Defense in Obama's first term, Robert Gates admitted in an interview, "'This is a terrible confession…I can't get a number on how many contractors work for the Office of the Secretary of Defense.'"[116]

Once money has transferred from the DoD into the private sector, the private sector then uses a portion of those funds to influence public policy through congressional lobbying. In the last ten years, the number of lobbyists for cybersecurity issues has exponentially increased. In a 2012 *Washington Post* article, reporter James Ball explains:

> In 2001, only four firms listed cybersecurity as an issue on which they were lobbying, according to a Washington Post computer analysis of congressional lobbyists filings. By 2006, this had risen to 129 and in 2011, the last full year of data available, 1,489 companies listed cybersecurity in disclosure forms required by Congress.[117]

By 2012, the number of companies listing cybersecurity as a focus point jumped to 1,968.[118] Among lobbyists were the same defense contractors benefitting from increased spending into cyber issues such as Raytheon and Lockheed Martin.[119]

The two biggest recipients of campaign funds from defense contractors totaling a combined $433,000, Senator Dick Durbin (D-IL) and Senator John Cornyn (R-TX), have both supported or sponsored legislation focused on cybersecurity issues. For example, Senator Cornyn's sponsored and passed amendment to the National Intelligence Reform Act of 2004 mandates that "federal agency heads make cybersecurity a priority when procuring new IT equipment."[120] This type of amendment might

---

[116] Priest, Dana, and William Arkin. 2014. "National Security Inc." *The Washington Post*. Accessed February 1. http://projects.washingtonpost.com/top-secret-america/articles/national-security-inc/.
[117] Ball, James. 2012. "Good News for Lobbyists: Cyber Dollars." *The Washington Post*, November 13. http://www.washingtonpost.com/postlive/good-news-for-lobbyists-cyber-dollars/2012/11/12/158a361e-29f9-11e2-b4e0-346287b7e56c_story.html.
[118] Pepitone, Julianne. 2013. "Cybersecurity Lobbying Doubled in 2012." *CNNMoney*. April 8. http://money.cnn.com/2013/04/08/technology/security/cybersecurity-lobbying/index.html.
[119] Engleman, Eric, and Jonathan D. Salant. 2013. "Cybersecurity Lobby Surges as Congress Considers New Laws." *Bloomberg*. March 21. http://www.bloomberg.com/news/2013-03-21/cybersecurity-lobby-surges-as-congress-considers-new-laws.html.
[120] "John Cornyn - United States Senator for Texas." *Senator Cornyn's Legislative Efforts*. http://www.cornyn.senate.gov/public/index.cfm?p=ScienceTechnology.

appear harmless, but when only the top defense agencies can guarantee secure equipment the amendment then becomes a way to edge out new competitors.

In addition to the exchange of money, there are two main transfers of personnel between the private and public industry. The first is between civilian federal employees and the private defense industry and the second is between former military personnel into the private defense industry.

Moving between the public and private sector is a normal career choice for many employees. In doing so, it helps to strengthen the ties between the public and private sector. Proving that contracts are explicitly secured for the private industry by former private workers now in government positions is beyond the scope of this thesis. However, there is enough evidence to accurately show that there is indeed a relationship between the two industries when it comes to cyber issues. I will highlight a few key individuals as evidence of a widespread pattern of the revolving door between private and public industry.

James Clapper, the current Director for National Intelligence since 2010, has spent the last twenty years bouncing between government and private institutions. Since retiring from the Air Force in 1995, Clapper has worked for Booz Allen, SRA International, Geospatial-Intelligence Agency, and DFI International in that order. Mike McConnell, Clapper's predecessor, is now a vice chairman of Booz Allen where he was brought on to coordinate Booz Allen's cyber efforts.[121] Booz Allen has a particularly close relationship with the federal government. CNN reports that in 2012, "Company filings show that 99% of Booz Allen's revenue comes from various levels of the federal government."[122] Undoubtedly, Booz Allen has everything to gain from continuing its close ties to those in power.

As further proof of a close connection between public and private sectors in relation to cyber security, Booz Allen's Chairman and Chief Executive Officer, Dr. Ralph W. Shrader, is a past federal employee formerly working at the US National Communications System and Defense Information

[121] "Booz Allen Hamilton Fiscal Year 2012 Annual Report." 2012. Fiscal Year Report. Booz Allen Hamilton. http://www.boozallen.com/media/file/Booz-Allen-FY12-annual-report.pdf. Pg 5
[122] Riley, Charles. "Booz Allen Hamilton in Spotlight over Leak." *CNNMoney*. http://money.cnn.com/2013/06/10/news/booz-allen-hamilton-leak/index.html.

Systems Agency working to setup and create secure network systems.[123] Melissa Hathaway, a former Booz Allen employee, then served as Senior Advisor to the Director of National Intelligence and Cyber Coordination Executive under McConnell.[124] [125]

Stephanie O'Sullivan, the Principal Deputy Director of National Intelligence (PDDNI) under James Clapper formerly worked at TRW, now a subsidiary of Northrop Grumman.[126] After leaving TRW she worked in the CIA for 15 years before being tapped by President Obama at the suggestion of James Clapper for the PDDNI position.

The second transfer between former military personnel and the private defense industry helps the defense industry to gain highly trained and knowledgeable employees. Defense contractors actively recruit former military personnel in order to fill their ranks. A third of Booz Allen's workforce is made up of former military personnel.[127] Booz Allen has even created transition programs in order to facilitate the process of moving from active duty to civilian life.[128] Lockheed Martin also recruits from the military, explaining on their website, "Our dedicated Military Relations team attended 270 transitioning military and veteran hiring events and participated in more than 60 transition assistance programs at military installations across the country in the past year."[129] Defense contractors benefit by recruiting form the ranks of past military personnel by attaining trained professionals that know the system and often-times come with high-valued security clearances.

---

[123] "Dr. Ralph W. Shrader." 2014. Booz Allen Hamilton Corporate Website. *Booz Allen Executive Leadership*. Accessed April 10. http://www.boozallen.com/about/leadership/executive-leadership/Ralph-Shrader.
[124] Borger, Julian. 2013. "Booz Allen Hamilton: Edward Snowden's US Contracting Firm." *The Guardian*, June 9, sec. World news. http://www.theguardian.com/world/2013/jun/09/booz-allen-hamilton-edward-snowden.
[125] "Melissa Hathaway." *Forbes*. http://www.forbes.com/profile/melissa-hathaway/.
[126] *Confirmation of Stephanie O'Sullivan to Be PDDNI*. 2011. Washington, D.C. http://www.fas.org/irp/congress/2011_cr/osullivan.html.
[127] "Transitioning Military". Booz Allen Hamilton Corporate Website. http://www.boozallen.com/careers/find-your-job/military.
[128] Ibid.
[129] "Military & Veteran Support". Lockheed Martin Corporate Website. http://www.lockheedmartin.com/us/who-we-are/community/customer.html.

Private contractors also recruit from universities. BAH has a "Cyber University partnership with University of Maryland University College."[130] BAH pays the University of Maryland to train and develop their employees' abilities. Employees are put through the program to gain additional DoD certifications that allow them to handle sensitive contracts. To date, 223 of their employees have either completed or are currently in the program.[131] BAH is not alone in looking to universities for trained employees. SAIC is also helping to fund cyber security programs at the University of Maryland.[132] The DoD similarly funds research at the University level, investing a total of $2.1 billion into university research in 2013.[133] Spending spent on cyber operations research then helps fuel an industry centered on the development of weapons.

Not every program focuses on cyber issues directly, but rather envelopes a wide-array of technical issues. Lockheed Martin funds a graduate program at the University of Colorado for Engineering Management.[134] The graduates then go work in teams focused on developing the infrastructure on which cyber operations function.

The system of continually finding funding is further fueled by the creation of an opposing force to fight against. Hence, the language used to describe cyber space largely centers on phrases that describe cyber events in war-like terms. Bruce Schneier often pushes against such a system as a creation of a false enemy in order to fuel the defense industry.[135] In his online blog post, Schneier explains why private

---

[130] "Booz Allen Hamilton Fiscal Year 2013 Annual Report." 2013. Fiscal Year Report. Booz Allen Hamilton. http://www.boozallen.com/media/file/Booz-Allen-FY13-annual-report.pdf. Pg 35.
[131] Ibid.
[132] Eckert, Barton. 2010. "SAIC Teams on Cybersecurity with University of Maryland." *Washington Business Journal*. November 1. http://www.bizjournals.com/washington/news/2010/11/01/saic-teams-on-cybersecurity-with.html.
[133] "United States Department of Defense Fiscal Year 2013 Budget Request." 2014. Budget Request 4-0609CA0. Washington, D.C.: The Department of Defense. http://dcmo.defense.gov/publications/documents/FY2013_Budget_Request_Overview_Book.pdf. Pg 4-10
[134] Melle, Carl. 2013. "CU-Boulder's Lockheed Martin Engineering Management Program Partners with IMC to Offer New Management Consulting Certificate." *University of Colorado Boulder*. April 22. http://www.colorado.edu/news/releases/2013/04/22/cu-boulder%E2%80%99s-lockheed-martin-engineering-management-program-partners-imc.
[135] Schneier, Bruce. 2014. "Tufts ALLIES Presents: Cybersecurity and Civil-Military Relations, A Lecture by Bruce Schneier". Lecture presented at the ALLIES, April 7, Tufts University. https://www.facebook.com/events/678939652148891/.

companies use the rhetoric of war to describe cyber events saying, "There is an enormous amount of money and power that results from escalating a cyber war arms race: power for the military, power for law enforcement and power for the large government contractors that support these organizations."[136]

Singer reinforces Schneier's claims explaining, "…cyber experts at George Mason University found extensive evidence of threat inflation in Washington, DC, cyber discussions, most frequently by those with political or profit incentives to hype the threats."[137] Centering the language used to discuss war mentalities helps to generate fear and maintain funding for defense contractors.

Opening up defense work to multiple contractors similarly opens up more points of vulnerability. In 2012, Chinese hackers broke into BAE computers and stole plans of the F-35 Lightning II fighter jet.[138] Lockheed Martin suffered a major cyber attack in 2011, though their I.T. personnel were able to cut off access to the attackers before any information could be taken.[139]

Unsuccessful attacks, like the one against Lockheed Martin, help support the use of contractors by creating an environment of ever-constant threat. The attacks prove that the use of contractors is warranted and that the private contractors are capable of defending themselves.

Within the last year there has been a strong push from congress to limit federal funding for defense spending, specifically highlighting the use of contractors. Clapper has since defended their use in a Congressional hearing and argued on behalf of contractors continued value. Legislative attempts to

---

[136] Schneier, Bruce. 2013. "Rhetoric of Cyber War Breeds Fear - and More Cyber War". Personal Blog. *Schneier on Security*. March 14. https://www.schneier.com/essay-421.html.
[137] Singer, Peter W.; Friedman, Allan (2013-11-16). Cybersecurity and Cyberwar: What Everyone Needs to Know (p. 165). Oxford University Press, USA. Kindle Edition.
[138] "Security Experts Admit China Stole Secret Fighter Jet Plans." 2014. *The Australian*. Accessed April 21. http://www.theaustralian.com.au/news/world/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154.
[139] Schwartz, Matthew. 2011. "Lockheed Martin Suffers Massive Cyberattack." *Dark Reading*. May 30. http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151.

reduce the salary cap of defense contractors from $763,000 to $230,700 have similarly been unsuccessful.[140]

Other high-ranking officials are trying to protect the cyber industry from budget cuts. Zachary Fryer-Biggs, writing for *Defense News* explains, "What is clear is that senior administration officials are attempting to shelter cyber from budget cuts, and even boost investment in the area."[141] I expect to see less money put towards the purchase of tanks, aircrafts, and massively expensive battleships in the near future and a portion of the reduced funds then put towards spending on cyber weapons.

In conclusion, the MDC is a rapidly growing source of money for the private sector supported by public funds. It will surely never replace the MIC but its growth and development will help those defense corporations currently in power maintain their sphere of influence over public policy. As the slew of systems governing war changes, so does the strategy involved in war making. In the next chapter, I will be discussing the evolving nature of warfare as it relates to cyberwar.

[140] Jilani, Zaid. 2013. "House Freezes Pay For Federal Workers, But Lets Defense Contractors Earn More Than Obama". Bold Progressives. http://boldprogressives.org/2013/02/house-freezes-pay-for-federal-employees-but-lets-defense-contractors-earn-more-than-president/.
[141] Fryer-Biggs, Zachary. 2013. "Cybersecurity Bubble Bursting for U.S. Contractors." *Defense News*. March 4. http://www.defensenews.com/article/20130304/DEFREG02/303040015/Cybersecurity-Bubble-Bursting-U-S-Contractors.

CHAPTER 5: THE EVOLVING NATURE OF WARFARE

1364 - First recorded use of a firearm
1892 - Automatic handguns
1912 - Creation of the warplane
1916 - Creation of the tank
1940s - Blitzkrieg tactics introduced
1945 - First test of a nuclear bomb
2000s - Creation of the railgun, weaponized viruses, cyber weapons, and drones.

The weapons of war have progressed into more efficient killing machines for thousands of years, making major strides in the past hundred years. Cyber warfare is the introduction of a new system of warfare and is the natural progression of humanity attempting to solve difficulties through eliminating the enemy. In this chapter, I will detail the main motive to go to war. I will then examine additional sub-reasons that a state would participate in a cyber campaign. Finally, I will end by outlining the various aspects that differentiate cyber war from past forms of war including the types of attacks, the involvement of troops, and the targets chosen for attack.

In her book, New and Old Wars, Mary Kaldor details the evolving goals of nations going to war. She summarizes that war in the 17th & 18th century was fought for "reasons of the state, dynastic conflict" or "consolidation of borders." War then evolved in the 19th century to settling "national conflict". In the early 20th century war went through another change to finally settle on resolving "national and ideological conflict". In the late 20th and early 21st century national conflict was shed from major reasons leaving "settling ideological conflict" as the main reason for going to war.

In terms of cyber warfare, ideological conflict undoubtedly plays a major role for going to war. Yet, it would be a mistake to assume ideological conflict is the main reason a state or non-state would want to launch *any* cyber attack. Other forms of warfare like troop mobilization or launching a missile would undoubtedly cause a corresponding escalation and cyber weapons can be used to accomplish a similar task with minimal risk of retaliation.

States have many possible reasons to launch a cyber military campaign. There are three major reasons that I will delve into further.

1. Gaining information to help the economic, technological, or political situation.

Major states are using cyber weapons in order to advance ulterior motives. The Chinese are especially prolific in the use of cyber weapons in order to gain an economic advantage. Laura Galante, a former Defense Intelligence Agency cyber specialist explains Chinese cyber tactics saying, "To the Chinese, this isn't first and foremost a military weapon, it's an economic weapon…"[142] A majority of Chinese cyber attacks are executed in order to improve the economic output of the state.

As discussed in chapter 2, Russian interests tend to follow a national extension of political power as in the case of Estonia, Georgia, and most recently, Ukraine.

2. Closing the technological gap between competing countries.

As aforementioned, China is infamous for using cyber attacks in rode to gain an economic advantage. Part of gaining an economic advantage has to do with pursuing a technological dominance over competitors. Breaking into the databases of research institutions and stealing their data cuts down costs and time allotted to doing the research from scratch.

3. National safety and promoting national interests.

The United States and its allies, along with the U.N., have been trying for years to somehow curb Iran from obtaining a nuclear weapon. Up until January of 2014, the U.N. had several active sanctions against Iran. Since 2006, the U.N. Security council has in acted four of such sanctions for its failure to abide by the International Atomic Energy Agency's demands.[143] These sanctions attempted to force Iran economically to reconsider its investment into nuclear power. During this time, the United States launched what is largely considered to be the most sophisticated cyber attack to date, now titled, Stuxnet.

[142] Sanger, David E. 2014. "U.S. Tries Candor to Assure China on Cyberattacks." *The New York Times*, April 6. http://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html.
[143] "Q&A: Iran Sanctions." *BBC News* 8 Nov. 2013. Web. 1 Oct. 2013.

Stuxnet was collaboratively developed by the United States and Israel. Specifically the worm "was created as part of a joint operation between the Israelis and the NSA's Foreign Affairs Directorate (FAD)."[144] Stuxnet attacked a key piece of Siemens' industrial technology that regulated the use of centrifuges in the Iranian uranium enrichment facility in Natanz. Stuxnet caused the controller to unnoticingly increase centrifuge speeds beyond regulated levels causing a higher rate of failure. Iran's facility operates by funneling uranium through a series of centrifuges. The technology is pre-current nuclear technology, but because of the sanctions against Iran, the Iranian government could not procure a more advanced system. Centrifuges naturally fail over time. Natanz is built to have redundant channels so that even if one centrifuge fails the enrichment process can still continue as engineers replace the failed centrifuge. Instead of trying to procure a more advanced system, Iran elected to simply accept that centrifuges were going to fail and replace them at a higher rate at which they broke down. Thus, when Stuxnet increased the rate at which centrifuges failed then the effect was to slow down the entire enrichment process, severely impeding Iran's ability to enrich uranium.

Brenner explains the impact of Stuxnet saying, "The attack was not a total success; it disabled about a fifth of Iran's nuclear centrifuges but left the rest unharmed. It was successful enough, however, to delay Iran's nuclear weapons program by about five years."[145] The worm has been in operation since its initial release in 2005.[146]

When the security firm Symantec first revealed the malware, researchers suspected that the software had been developed by the United States because of the unprecedented level of technical sophistication. John Markoff, writing for the New York Times, reported in 2010 about suspected government involvement saying, "The malware was so skillfully designed that computer security specialists who have examined it were almost certain it had been created by a government and is a prime example of

[144]Thomson, Iain. 2013. "Snowden: US and Israel Did Create Stuxnet Attack Code." *The Register*, July 8.
[145] Brenner, Joel. 2011. *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press. Pg 104.
[146]Thomson, Iain. 2013. "Snowden: US and Israel Did Create Stuxnet Attack Code." *The Register*, July 8.

clandestine digital warfare."[147] Until Edward Snowden leaked key documents detailing NSA coordination, it was still just a rumor that the U.S. was indeed behind the attack.

The United States could have approached Iran with threat of invasion or full-scale assault. However, this tactic would have been highly controversial and likely unsuccessful judging from past and current efforts in the Middle East. Instead, a concentrated, coordinated cyber attack was able to achieve what years of International politics were unable to complete. United States interests were aided through use of a stealth cyber attack without having to place any troops on the ground. Cyber attacks should be considered part of the United States arsenal for political diplomacy in order to achieve similar goals in other states. Liberal use of a cyber attack on allies would undoubtedly have major ramifications for U.S. International influence, but the coordinated use against opposition states could have a similarly positive net effect for national interests as in the case of Stuxnet.

Before the development of 21st century war, ideology could be pushed onto a population via national military campaigns. As Kaldor notes, in the new age of warfare military campaigns are no longer an effective method to pursue the spread of ideology. In the case of the wars in Iraq and Afghanistan, converting the Iraqi and Afghani people to democratic issues is proving harder than initially believed, especially when the military attempts to stabilize a country dominated by infighting and tribal war for thousands of years. Cyber attacks and cyber war is not a solution to spread ideology as the attacks are completely void of any ideological component.

As further proof, attributing the source of a cyber attack is exceptionally difficult. Cyber attacks do not come with a return address. In physical warfare identifying if a state is involved in warfare is fairly simple because of international standards; planes must have their tales painted to identify their origin; tanks are obvious examples of state involvement. Cyber weapons are not as easily identifiable because both states and non-states are using the same weapons. Even establishing the origin of the attack can be difficult.

[147] Markoff, John. 2010. "Stuxnet Worm Is Remarkable for Its Lack of Subtlety." *The New York Times*, September 26, sec. Technology. http://www.nytimes.com/2010/09/27/technology/27virus.html.

Cyber security expert, Bruce Schneier, predicts that states are probably using the same resources as non-states in order to add an additional layer of secrecy to their activities.[148]

A natural result of both states and non-states using the same weapon is the need for increased communication and transparency among states when launching a cyber attack. In an attempt to harm or frame states, non-state actors could unleash attacks that appear to originate from the state. Communication channels akin to the red phone between the U.S. and Russia in case of nuclear threat will help prevent hair-trigger cyber weapons from being accidentally unleashed.

The Obama administration is already attempting to open up these lines of communication with China. For the past several months, U.S. officials have met with their Chinese counterparts in order to be more transparent with U.S. cyber activities. David Sanger explains, "…the hope was to prompt the Chinese to give Washington a similar briefing about the many People's Liberation Army units that are believed to behind the escalating attacks on American corporations and government networks."[149] However, China has yet to provide a similar briefing to U.S. officials and does not appear to be moving any closer to a transparent cyber force. The United States is not in a position to develop similarly transparent relations with Russia because of heightened tensions over the annexation of Crimea and a still tense situation playing out in Eastern Ukraine.

The next component of war that cyber war changes is the use of troops. Cyber troops are now coders, network operators, technicians, and command and control operators that are actively creating and monitoring cyber weapons as well as the accompanying infrastructure. Already we are seeing the influx of vastly increased distance fighting. Meaning, a drone operator sits in a base in the Midwest United States can operate a drone in the Middle East in real time. Cyber weapons build on that development through the use of so called cyber warriors or cyber troops.

---

[148] Schneier, Bruce. 2014. "Tufts ALLIES Presents: Cybersecurity and Civil-Military Relations, A Lecture by Bruce Schneier". Lecture presented at the ALLIES, April 7, Tufts University. https://www.facebook.com/events/678939652148891/.

[149] Sanger, David E. 2014. "U.S. Tries Candor to Assure China on Cyberattacks." *The New York Times*, April 6. http://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html.

On a theoretical level, cyber troops can operate from virtually any location with Internet access. On a more practical level, they tend to be located in major U.S. military bases such as the one in Fort Meade, MD or one of the several scattered across the country. The distance created between the troops and the target will undoubtedly have a major impact on troop readiness and the effect of combat related stress on troops.

Additionally, in order to prepare for wartime, cyber troops will not be required to travel fast distances in order to fight the enemy. The lack of travel time fundamentally increases the speed of war as attacks can be launched in rapid succession without the need to physically relocate key infrastructure. Furthermore, launching attacks from afar saves the state on troop maintenance costs. According to report done by the Center for Strategic and Budgetary Assessments, each troop in Afghanistan in 2014 costs $2.1 million per.[150] For context, the cost was formerly found to be under $1.3 million a year for all the previous years.[151]

Perhaps most impactful for troops is the effect of cyber weapons on combat stress. Combat related stress has made a huge change in troop morale and public perception of war. In both the War in Vietnam and the War in Afghanistan the number of military suicides has surpassed the number of combat deaths. As the wars in the Middle East draw to a close, combat related deaths are on the decline while active-duty suicides are steadily increasing.[152] The constant stress of wartime slices like a wound across the psyche of a soldier, affecting him or her far beyond the physical confines of war.

Cyber war offers no such close combat that could cause intense emotional harm to the troop. Attacks can be safely launched from the safety of American soil. The gore and brutality of killing is totally absent from a cyber attack. One of the major features of a cyber war is that there are not necessarily objects

---

[150] Krumboltz, Mike. 2013. "It Costs $2.1 Million per Year for Each Soldier Deployed in Afghanistan: Report." *Yahoo News*. October 25. http://news.yahoo.com/it-costs--2-1-million-per-year-for-each-soldier-deployed-in-afghanistan--report-133150602.html.
[151] Ibid.
[152] Friedman, Brandon. 2013. "Military Suicides Top Combat Deaths - But Only Because The Wars Are Ending." *Time Magazine*, January 16. http://nation.time.com/2013/01/16/military-suicides-top-combat-deaths-but-only-because-the-wars-are-ending/.

blowing up because of a missile strike or bombing raid. Instead, facilities simply do not work. The power to hospitals is shut down, traffic lights malfunction, and air traffic controllers are unable to track active flights. Surely, in the aforementioned cases many people will be hurt as a by-product of the attack - but not as a direct result. The high level of suicides as a result of combat stress will undoubtedly decline in the use of cyber troops.

The next change as a result of increased cyber attacks is the impact of collateral damage. Collateral damage is an intentionally vague term to describe the unintended consequences of an attack. Cyber weapons fundamentally change the nature of collateral damage by vastly expanding the possible area for unintended damage to occur.

In the case of Stuxnet, the malware spread far beyond the intended target. John Markoff explains, "As in real warfare, even the most carefully aimed weapon in computer warfare leaves collateral damage."[153] In the realm of cyber warfare that fact not only remains true, but is epitomized ten-fold. In the physical world, collateral damage as a result of a drone strike is isolated to the immediately surrounding area or a misidentified target whereas a cyber attack can spread literally worldwide.

Farwell and Rohozinski, speaking in reference to Stuxnet, explain the effect of collateral damage saying, "Although code can be designed to hit a specific target, in practice, once launched, there was no control over the consequences it inflicted - or upon whom."[154] The U.S. and Israeli forces designed Stuxnet to target Iranian nuclear facilities, but the malware spread well beyond Iranian facilities. Just under 60% of infected computers were in Iran.[155] The rest of the computers were spread throughout Indonesia, India, Azerbaijan, and even in the United States. Singer explains, "Stuxnet was specifically tailored to target just a few Iranian centrifuges and yet ended up spreading to well over 25,000 other

---

[153] Markoff, John. 2010. "A Silent Attack, but Not a Subtle One." *The New York Times*, September 26, sec. Technology. http://www.nytimes.com/2010/09/27/technology/27virus.html.

[154] Farwell, James, and Rafal Rohozinski. 2012. "The New Reality of Cyber War." *Survival: Global Politics and Strategy* 54 (4): 107–20. doi:10.1080/00396338.2012.709391.

[155] "W.32 Stuxnet." 2010. Threat Analysis. *Symantec*. July 13. http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

computers around the world."[156] Fortunately, in the case of Stuxnet, the worm was virtually harmless to everyday computers as it was specifically designed for the Natanz facility. Since most people do not own a Siemens nuclear centrifuge, the attack was rendered moot.

One argument against the possibility of increased collateral damage in the cyber world is evidence that Stuxnet damaged no other enrichment facilities. However, code can sometimes go awry. For example, Stuxnet was not supposed to spread beyond Iran, yet an update to the software made it spread faster and ultimately led to its discovery. Despite the high level of technical skill the United States and its allies have at their disposal, mistakes can be made that extend far across the global spectrum.

The risk of collateral damage is increased for a cyber attack because the enemy's military is no longer the optimal target. In modern warfare, civilians are outside the list of available options for states to target. Civilians living in war zones will undoubtedly have a higher chance of being caught in the crossfire, but the civilians cannot be the target of the attack. The fourth treaty of the Geneva Convention, ratified in 1949, lays out key civilian protections during wartime. The fourth treaty goes so far as to mandate the establishment of neutral zones for non-combatants to gather for protection and humanitarian services.[157]

Thus far, cyber warfare does not follow the same convention. Russia's attack on Estonia shutdown the entire state's economic, politic, and business industry. Stuxnet specifically avoided any military operations and aimed straight for Iran's research and energy industry.[158] Attacks against Google and Microsoft appearing to originate from China are specifically targeting the technological infrastructure of the United States. In the case of cyber warfare, targets will also include power transformers and phone lines in order to induce a virtual fog of war. When Russia invaded Crimea in 2014 they physically

---

[156] Singer, Peter W.; Friedman, Allan (2013-11-16). Cybersecurity and Cyberwar: What Everyone Needs to Know (Kindle Locations 2469-2470). Oxford University Press, USA. Kindle Edition

[157] "ICRC Databases on International Humanitarian Law." 1949. *Treaties and State Parties to Such Treaties*. August 12. http://www.icrc.org/ihl.nsf/385ec082b509e76c41256739003e636d/6756482d86146898c125641e004aa3c5.
Part II, Article 15, (b).

[158] I realize one could argue that the nuclear facility could also be a military facility.

stormed the phone lines and shut down all communication within the region. In the United States private industry controls much of the electronic, Internet, and communication infrastructure and, as a result, be a primary target in the case of cyber warfare.

In 2013, the Syrian Electronic Army (SEA) hacked Twitter, the New York Times, and the Washington Post in retaliation for possible U.S. involvement in Syria. The hackings took on a different character when the SEA began releasing false reports about explosions in the White House, which then caused markets to drop.[159] Paul Farhi and Hayley Tsukayama writing for the Washington Post explain, "The message sent the stock market into a panic, causing the Dow Jones industrial average to lose more than 100 points within two minutes."[160] While it cannot be proven whether the SEA was simply playing a prank, sending a threat, or intentionally trying to impact the U.S. economy, the effect of the point drop cannot go unnoticed by hackers that seek to hurt the U.S. We should expect that future cyber attacks will be similarly aimed at making a significant economic impact.

Martin Van Creveld, Israeli war historian explains, "The news that present-day armed violence does not distinguish between governments, armies, and peoples will scarcely surprise the inhabitants of Ethiopia, the Spanish Sahara, or - to select an example from the developed world - those of Northern Ireland."[161]

As civilians increasingly becomes the target of cyber attacks, the populace involved in war efforts will blend between combatants and non-combatants. Cyber attacks will push warfare into civilian life and encourage more civilians to get involved in war efforts. As discussed in Chapter 2, non-state actors working independently, on behalf of the state, or with a loose connection with the state is on the rise.

---

[159] Waterman, Shaun. 2013. "Syria, Iran Armed for Cyberwar with U.S." *The Washington Times*, August 28. http://www.washingtontimes.com/news/2013/aug/28/syria-iran-capable-of-launching-a-cyberwar/.
[160] Farhi, Paul, and Hayley Tsukayama. 2013. "Syrian Electronic Army Hacks Washington Post Web Site." *The Washington Post*, August 15, sec. Lifestyle. http://www.washingtonpost.com/lifestyle/style/syrian-group-hacks-washington-post-web-site/2013/08/15/4e60d952-05bd-11e3-88d6-d5795fab4637_story.html.
[161] Creveld, Martin Van. 1991. *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*. 1St Edition edition. New York : Toronto : New York: Free Press. http://www.amazon.com/Transformation-War-Reinterpretation-Conflict-Clausewitz/dp/0029331552/ref=sr_1_3?s=books&ie=UTF8&qid=1398107581&sr=1-3. Pg 58.

While he did not specifically highlight cyber warfare as a rising field, he did target the underlying nature of war explaining, Van Creveld explains further, "As new forms of armed conflict multiply and spread, they will cause the lines between public and private, government and people, military and civilian, to become as blurred as they were before 1648."[162] As the entry level for technology drops we should expect to see more non-state actors involved in war making and war profiteering in the cyber world.

When characterizing new wars of the late 20th century and early 21st century, Kaldor notes that there are five main types of troops involved in war. Those troops are "regular armed forces or remnants thereof; paramilitary groups; self-defense units; foreign mercenaries; and finally, regular foreign troops, generally under international auspices."[163] The big question is, given Kaldor's framework, how do we categorize non-state hackers that organize apart from the state but toward state ideological interests?

In truth, Kaldor's categories do not account for cyber actors. However, by acknowledging the intent of the self-defense units then the hackers and hacktivists could be classified as self-defense units to fit within her model. Kaldor's description rests almost exclusively on the assumption that the groups are physically defending their localities, instead of operating through a cyber medium.

The non-state actors that are paid by the state could be easily classified in Kaldor's paramilitary group. Kaldor describes the physical traits of the group saying, "They rarely wear uniforms, which makes them difficult to distinguish from non-combatants…"[164] The same sense of underground activity that Kaldor describes the physical make-up of the paramilitary troops also characterizes the blending of combatants and non-combatants in the cyber world. As Van Creveld explained earlier, the distinction between combatants and non-combatants is only becoming more vague in the new war paradigm.

---

[162] Creveld, Martin Van. 1991. *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*. 1St Edition edition. New York : Toronto : New York: Free Press. http://www.amazon.com/Transformation-War-Reinterpretation-Conflict-Clausewitz/dp/0029331552/ref=sr_1_3?s=books&ie=UTF8&qid=1398107581&sr=1-3. Pg 226.

[163] Kaldor, Mary. 2007. *New and Old Wars: Organized Violence in a Global Era, Second Edition*. 2nd Edition. Stanford, Calif.: Stanford University Press. http://www.amazon.com/New-Old-Wars-Organized-Violence/dp/0804756465/ref=sr_1_3?s=books&ie=UTF8&qid=1398021599&sr=1-3&keywords=mary+kaldor+new+and+old+wars. Pg. 97.

[164] Ibid. Pg 99.

Historically war mobilization has taken weeks, if not months to mobilize troops. When Russia agreed go to war in WWI, it took six weeks for Russia to mobilize its troops. Germany believed it could take France in WWI in 45 days. Cyber attacks occur in a millisecond. In a lecture at Tufts, Bruce Schneier explains that cyber attacks happen in a millisecond and governments struggle to react fast enough to attacks.[165] Jason Shackleford, quoting the White House National Strategy to Secure Cyberspace, notes in his review of cyber warfare that, "The speed and anonymity of cyber attacks makes it difficult to distinguish among "the actions of terrorists, criminals, and nation states.""[247]

Clearly the United States needs reform if it is to compete in cyberspace. The major area in need of reform is in the policies surrounding the use of cyber attacks. In the next chapter, I will introduce the current legal framework for cyber issues as well as discuss the complications surrounding the lack of internationally recognized cyber laws.

[165] Schneier, Bruce. 2014. "Tufts ALLIES Presents: Cybersecurity and Civil-Military Relations, A Lecture by Bruce Schneier". Lecture presented at the ALLIES, April 7, Tufts University. https://www.facebook.com/events/678939652148891/.

CHAPTER 6: THE LAWS THAT GOVERN CYBER OPERATIONS

"No universally accepted legal framework for dealing with cyber threats exists."[166] - The Organization for Cooperation and Security in Europe.

Creating a unified cyber framework is exceedingly difficult because it requires virtually every state to cooperate on the same standard. China, Russia, the United States would especially need to agree in order to build the smallest coalition needed to bring about major change. Unfortunately, they are also the furthest when it comes to agreeing on a similar cyber standard.

In this chapter I will introduce the obfuscated legal framework and arguments surrounding all forms of cyber warfare. I will begin by explaining some past efforts and will move from there to discuss how international law has been adapted to apply to cyber space. Finally, I will introduce the current laws that specifically relate to cyber space as well as my recommendations on whether or not cyber warfare necessitates a treaty of its own.

Cyber space is still a relatively new domain for warfare and the laws surrounding its appropriate use are still being formulated. Writing for the Strategic Studies Institute for the U.S. Army War College, Keir Giles and Andrew Monaghan explains:

> While there is a broad agreement among the United States and its allies that cyber warfare would be governed by existing law of armed conflict, with no need for additional treaties or conventions to regulate hostilities online, this view is not shared by many nations that the United States could potentially face as adversaries.[167]

The United States believes international doctrine can already be applied to cyberspace so no new treaty is necessary.[168] However, cyber space, like all new modalities of warfare, requires some clarification rather than clumsy adaption of old laws. Jeffrey Carr explains:

> Right now, no comprehensive international treaty exists to regulate cyber attacks. Consequently, states must practice law by analogy: either equating cyber attacks to traditional armed attacks and

[166] Giles, Keir, and Andrew Monaghan. 2014. "Legality In Cyberspace: An Adversary View". U.S. Army War College Strategic Studies Institute. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1193.pdf. Pg 5.
[167] Ibid. Pg 5.
[168] Ibid. Pg 5.

> responding to them under the law of war or equating them to criminal activity and dealing with them under domestic laws.[169]

When international hackers are dealt with under domestic laws instead of international laws, several confounding issues follow. Namely, if the specific location of the attacker is discovered, does he or she happen to be operating in an allied state with an extradition agreement with the U.S? If not, is there an international legal doctrine that the United States can use to force extradition?

Attempts to create a unified international doctrine further highlight the rift between Western and Eastern cyber mentalities. The United States and its NATO and EU allies tend to agree on similar cyber doctrine. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence called on an International consort ion of scholars to produce a manual on how state cyber activities should be interpreted in the context of current international law. In 2013, the "International Group of Experts" released the Tallinn Manual; a 200-page document that equates cyber attacks to traditional physical attacks and then applies law precedent to those activities. Of interesting note, of all the legal experts there was not one Chinese or Russian contributor.

It is no wonder that in 2011 a team of Russian, Chinese, Tajikistani, and Uzbekistani "experts" submitted their own proposal to the U.N. though it has yet to be signed by any other countries. On the surface, the International Code of Conduct in Cyberspace (ICCC) appears to embody the very actions that would benefit every member of the U.N. States that voluntarily sign the agreement must work to "cooperate in combating criminal and terrorist activities which use ICTs including networks, and curbing dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability."[170] States must also work towards transparent management of the Internet and must agree to seek out peaceful means to resolving any conflict over Internet resources.

---

[169] Sklerov, Matthew. 2010. *Cyber Warfare*. 2nd Edition. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, Inc. Pg 47.

[170] "China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations." 2011. *Embassy of the People's Republic of China in New Zealand*, September 13. http://nz.chineseembassy.org/eng/zgyw/t858978.htm.

Yet, when viewed beyond surface analysis, deep-rooted issues regarding the laws of cyberspace come to light. Eastern and Western interpretations of cyber actions are variant enough to cause additional problems if a treaty were developed. For example:

> At a UN disarmament conference in 2008, a Russian Ministry of Defence representative suggested that any time a government promoted ideas on the Internet with the intention of subverting another country's government, including in the name of democratic reform, this would qualify as "aggression" and an interference in internal affairs. Yet at the same time, this is not construed by Sweden as a hostile act.[171]

The vagueness of the law and ability for various parties to interpret actions under state contexts can give rise to a series of possible vulnerabilities. In his blog, Carr points out several fundamental issues with the ICCC and calls it "a red herring" that "is part of an overall strategy of misdirection by China, Russia and the two former states of the Soviet Union."[172] The agreement would provide a legal justification to eliminate individual rights in return for protecting state rights. Individuals that appear to be controversial to the state can be blocked online. Finally, the treaty calls for a slow down on the development of cyber warfare capabilities while Russia and China are both ramping up their resources to their own cyber forces.[173] Clearly, fundamental issues regarding the discrepancy involving how each country interprets laws must be resolved before any meaningful international cyber treaties are enacted. Without new doctrine, states must rely on previous treaties to enforce state cyber actions.

The U.N. Charter in Articles 2(4) and 51 dictates two of the major components governing fair use of force on an international level. Seeing as the charter was written in the 40s, there is no way the authors of the U.N. Charter could have foreseen the rise of cyber conflicts. Yet, it is one of the main governing statues used to control the extent of war and must be examined to see if cyber attacks are in anyway limited by International law.

---

[171] Giles, Keir, and Andrew Monaghan. 2014. "Legality In Cyberspace: An Adversary View". U.S. Army War College Strategic Studies Institute. Pg 16.
[172] Carr, Jeffrey. 2011. "Digital Dao: 4 Problems with China and Russia's International Code of Conduct for Information Security". Security Blog. *Digital Dao*. http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html.
[173] Ibid.

Article 2(4) reads:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[174]

And Article 51 reads:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[175]

As seen above, Article 2(4) loosely outlines the legal limits of state involvement in another state's affairs. Article 51 provides the legal justification necessary to launch a self-defense strike in response to an "armed attack." States can only use force when either A) authorized to do so by the U.N. Security Council or B) in self-defense. As demonstrated from the previous chapters, cyber attacks have been used by states and non-states outside of these two possibilities without international ramification.

When discussing the territorial integrity of a state, cyber attacks skirt along blurred lines. Physical attacks like missiles and drone strikes have a clearly identifiable physical component associated with their use. Thus, if a state were to launch missiles against the United States then the U.S. could respond by invoking Article 2(4) and Article 51 of the U.N. Charter as legal justification to defend itself.

Thus far, despite the plentiful amount of cyber attacks, a state has yet to be charged in violation of either of the aforementioned articles as a result of a cyber attack. The massive amounts of cyber espionage from China, the coordinated strikes against Iranian nuclear facilities, Russian DDoSing of Estonia and Georgia, have all gone unpunished by the United Nations.

The fact that no country has been brought before the U.N. to answer for these attacks is perhaps telling of the either inability or lack of will to establish a legal cyber precedent. Lack of clarity surrounding

---

[174] "Charter of the United Nations: Chapter I: Purposes and Principles." http://www.un.org/en/documents/charter/chapter1.shtml.
[175] Ibid.

cyber laws allows states to make major moves unimpeded without having to worry about legal international ramifications.

In regards to the word "force" used in article 2(4), Farwell and Rohozinski point out, "…'force' is not defined. There is no international convention that defines whether the use of software code should be deemed equivalent to the use of force."[176] The U.N. or other international bodies have yet to clarify or outline the use of force in cyber space. Doing so would be a strong step towards outlining a well-understood cyber law. As the Russian representative of the defense minister said earlier in the chapter, it would interpret another state's suggestions for "democratic reform" as an "act of aggression" - but not of force.

One question that goes unanswered in the articles is where does intent factor into assessing whether or not a cyber attack can be accurately categorized as a use of force? If so, Farwell and Rohozinski also note that, "…the US government apparently did view *Olympic Games*[177] as a use of force. The strategic objective was not only to retard Iran's progress in developing nuclear weapons, but to persuade Israel that using cyber weapons mooted the need for a kinetic attack on Tehran's nuclear institutions."[178] Of course, without an official statement released by U.S. Government it is nearly impossible to verify exactly what were the United States' intentions.

Intent is important for acknowledging violations of the U.N. Charter. Developing software to be effective can be a stumbling process. Oftentimes software requires tweaking, testing, and re-tweaking and retesting. If a state launches a cyber attack akin to Stuxnet but the attack is ultimately unsuccessful at achieving its end goal, then can the state be held in violation of the use of force? This is a question that will need to be reconciled on an international level in order to deter possible state orchestrated cyber attacks. So long as a cyber attack is not in violation of any international law then they can continue

---

[176] Farwell, James, and Rafal Rohozinski. 2012. "The New Reality of Cyber War." *Survival: Global Politics and Strategy* 54 (4): 107–20. doi:10.1080/00396338.2012.709391. Pg 111.

[177] The Olympic Games was a cyber operation run by the United States to interfere with Iran's ascertainment of nuclear weapons.

[178] Farwell, James, and Rafal Rohozinski. 2012. "The New Reality of Cyber War." *Survival: Global Politics and Strategy* 54 (4): 107–20. doi:10.1080/00396338.2012.709391. Pg 111.

unabated. Creating an example of a country using international policy could serve as a deterrent to other countries looking to launch cyber attacks.

State created cyber attacks that are clearly intended to cause significant damage to a state's political, economic, or military industry should be treated as violations of the use of force. To draw a physical world comparison, if North Korea launched dud ballistic missiles into South Korea, that action would readily be interpreted as an inappropriate use of force and cause for South Korea to invoke world protection. A cyber attack should be treated no differently and be subject to U.N. review and sanctions against the infringing country. Especially when we consider the recommendation of the International instate for Strategic Studies in which it concluded in 2010 that future international battles will likely include, "the use of cyber-warfare to disable a country's infrastructure, meddle with the integrity of another country's internal military data, try to confuse its financial transactions or to accomplish any number of other possibly crippling aims."[179] Failure to adopt a reliable framework to assess cyber attacks and larger cyber conflicts will result in the adaptation of old laws subject to uncharacteristic interpretations and thereby loose legal doctrine surrounding cyber engagements.

For example, a cyber attack may not violate Article 2(4) or Article (51) but it does violate Resolution 26/25 adopted in 1970 stating:

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.[180]

As discussed in previous chapters, cyber attacks are aimed either at the military, political, industrial, or economic system of the victim state. The broadness of the resolution allows for cyber attacks to be interpreted as "interference" with any of the elements included in the resolution. The resolution does not directly cite cyber issues but its vagueness lends itself to be adapted to the new conflict area.

---

[179] Waxman, Matthew. 2011. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *The Yale Journal of International Law* 36: 421 – 459. Pg 423.

[180] *2625 (XXV). Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations*. 1970. http://www.un-documents.net/a25r2625.htm.

Of important note is that the broadness of Resolution 26/25 also incriminates much of the United States' non-cyber activity and has yet to be used against the U.S. for its activities post 1970 including: financing Syrian revolutionaries, helping to bomb Gaddafi forces in 2011, lending aid to the coup in Venezuela in 2002, or supporting Afghani Mujahideen forces between 1979 and 1989. Seeing as the United States has yet to be proven in violation of Resolution 26/25 for its past activities, the U.N. has a very weak case for applying the resolution to U.S. cyber activities.

Somewhat ironically, the argument that can be used to support U.S. military intervention in Iraq, Afghanistan, and Pakistan is found within the same resolution in which it states:

> Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.[181]

When a state knowingly harbors international terrorists or is acquiescent in taking steps to eliminate said terrorists then it is in violation of Resolution 26/25 and other members of the U.N. can take necessary steps in order to eliminate the threat by invoking Article 51. As of yet, the resolution has yet to be used as legal precedent in order to engage non-state cyber actors that have acted against a member state. For example, no state has challenged Russian non-state involvement in the attacks against Estonia or Georgia. Similarly, no state has challenged China for its infamous harboring of an abundance of Chinese non-state cyber actors.

Probable causes for failure of the U.N. to find any state in violation of the resolution most likely centers around 1) Veto power of the U.S., Russia, and China, and B) Unwillingness of any member state to challenge one of the super powers or C) Failure to find reliable proof of cyber activities. Cyber states do not typically have Edward Snowdens or Chelsea Mannings that steal and leak an abundance of information to the global population in order to prove whether an activity was truly orchestrated by the non-state actors. In the future, the most likely time that this resolution could be used to justify sending troops into a state harboring cyber criminals is if those criminals launch major coordinated attacks against

[181] Ibid.

at least two super powers and operate in a non-super power state. However, this scenario is unlikely to occur for a number of reasons.

A non-state actor capable of launching a significant attack against two super powers would probably need state support or the financial resources equal to that of a small state. Given those resources, they are likely to use the shroud of cyber space to hide their origin. Finally, a state would most likely then not go straight to the U.N. with evidence because it would potentially tip off the cyber actors and instead the state would use an operation akin to the 2011 assassination of Osama Bin Laden in Operation Neptune Spear. A physical ground operation would reduce the possibility of the cyber actors escaping and moving underground.

NATO can also play a key role in enforcing international legal standards. In the case of the Russian attacks against Estonia, Shackledford reports, "the attacks were so widespread and the results so grave that Aaviksoo considered invoking Article 5 of the North Atlantic Treaty Organization ("NATO"), which states that an assault on one allied country obligates the alliance to attack the aggressor."[182] Though the former Minister of Defense did not end up requesting aid, this would have been the first time Article 5 had been invoked to protect against a cyber attack. Even the consideration demonstrates that states involved in future cyber wars could look at Article 5 as an option for rallying allies for military support.

Shackleford concludes that there are ultimately two options for the international community: "create a new treaty system from whole cloth, or adapt current treaty regimes."[183] He goes on to argue on behalf of creating a new treaty entirely focused on cyber issues.

Enforcing antiquated laws in the cyber world is a losing scenario for the international community. The legal framework as it stands is not capable of being adapted to enforce cyber laws because of the total originality of cyberspace. As demonstrated in Article 2(4) and Article 51 of the U.N. Charter, the laws were simply made in a different period of warfare. Attempts to reinterpret them will prove cumbersome

[182] Shackelford, Scott. 2009. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (1): 191–250. Pg 193.
[183] Shackelford, Scott. 2009. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (1): 191–250. Pg 197.

and only obfuscate the true protocol surrounding the legality of cyber warfare. Instead, a new treaty around cyber laws would make clear the technical framework by explicitly detailing what is and is not allowed under the new legal doctrine.

Informed parties should be trusted to create new cyber policies. Fortunately, the recent leaks by Edward Snowden have allowed for the average citizen to suddenly become very well informed regarding U.S. cyber actions. Unfortunately, the leaks have also led to a wealth of blowback against the United States. In the next chapter I will discuss the major revelations and resulting blowback against the United States.

CHAPTER 7: BLOWBACK AGAINST THE UNITED STATES

For every policy there are consequences. As a direct result of U.S. government intervention and activity in the cyber world, several U.S. based companies have experienced economic backlash from the world economy in the form of lost contracts, reneged businesses partnerships, missed potential sales, and loss of political influence. These losses are referred to as blowback and are the subject of this chapter.

The United States has received blowback for several major incursions including the war in Afghanistan, Iraq, and Vietnam, as well as for helping to overthrow several governments. In the last year, blowback as a result of U.S. cyber policy has cost the U.S. economy billions of dollars and is predicted to only grow larger throughout the rest of the decade.[184] In this chapter I will discuss the major revelations, the immediate and long-term blowback, and will then recommend possible courses of action for the United States to recover economically, politically, and socially from the losses. I have broken the chapter into three major parts to address various portions of the response.

Part I - Major Revelations and the Immediate Response from Allies and Affected Parties

Major revelations of U.S. cyber policy are a result of leaks from former defense contractor Edward Snowden. In 2013, Edward Snowden packed his bags and caught a plane to Hong Kong, China. While in China, Snowden revealed that he had 1.7 million scraped files that expose detailed secret activities of the National Security Agency. Before U.S. officials could revoke his passport, Snowden relocated to Russia where he applied for asylum and has been living ever since. Snowden released the trove of files to several journalists, most notably Glenn Greenwald working at The Guardian and Barton Gellman working at The Washington Post. For the past nine months, reporters have been slowly combing through the files to publish those that are deemed safe enough to be released. The steady stream of articles have included never-before mentioned NSA programs such as, PRISM, XKeyscore, Tempora, and several other formerly unheard of operations.

[184] Miller, Claire Cain. 2014. "Revelations of N.S.A. Spying Cost U.S. Tech Companies." *The New York Times*, March 21. http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

These revelations address the precursor to warfare - intelligence gathering. Without accurate intelligence, conducting cost-effective warfare would be impossible. Since the leaks began, the United States and the remainder of the Five Eyes[185] have received widespread International blowback.

Brazil's President Dilma Rousseff is one of the greatest proponents of anti-U.S. policies stemming from the recent leaks. In late 2013, leaked NSA documents revealed that the NSA had eavesdropped on the Brazilian President's phone calls. Since then, President Rousseff has systematically moved to cut off ties between Brazil and the United States economically, technologically, and politically. In September, 2013, just days after learning about the revelation, she gave a scathing speech against U.S. cyber efforts in front of the U.N. general assembly.[186] In her speech she called on the U.N. to pursue an organized policy to regulate state electronic activities, with specific reference to the United States.

Later that same year, just as Brazil was poised to announce a $4 billion deal with Boeing to build its F/A-18 Super Hornet fighter jets, President Rousseff changed direction and instead announced the contract to the German company, Saab.[187] The impact of losing the contract cannot be overstated. Brazil is currently poised as an emerging global market. The United States has spent countless man-hours strategically placing itself in line to guarantee a successful U.S. contractor. Even the White House got involved in 2013 to secure the deal. Brian Winter of Reuters explains, "After Biden's reassurances that the United States would not block crucial transfers of technological know-how to Brazil if it bought the jets, [President Rousseff] was closer than ever to selecting Chicago-based Boeing to supply its fighter, the F/A-18 Super Hornet."[188] Whoever gained the contract would also gain a strategic military and economic ally leading into the 21st century. Furthermore, the $4 billion would profoundly increase the financial and

---

[185] Australia, Canada, New Zealand, the United Kingdom, and the United States

[186] York, Julian Borger New. 2013. "Brazilian President: US Surveillance a 'Breach of International Law.'" *The Guardian*, September 24, sec. World news. http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

[187] Winter, Brian. 2013. "Insight: How U.S. Spying Cost Boeing Multibillion-Dollar Jet Contract." *Reuters*, December 20. http://www.reuters.com/article/2013/12/20/us-boeing-brazil-insight-idUSBRE9BJ10P20131220.

[188] Winter, Brian. 2013. "Insight: How U.S. Spying Cost Boeing Multibillion-Dollar Jet Contract." *Reuters*, December 20. http://www.reuters.com/article/2013/12/20/us-boeing-brazil-insight-idUSBRE9BJ10P20131220.

technological advantage of the company in order to gain key advantages leading to further possible contracts.

The Snowden revelations demolished all possibility of Boeing securing a contract and subsequently resulted in a strategic loss of a potentially major ally.

President Rousseff is also working with legislators to produce major legislation in the Brazilian National Congress that would impede the United States' ability to collect data.[189] The legislation would force U.S. companies to store all cloud data on servers located in Brazil, and not in the U.S. as currently in place. President Rousseff is also working with ISPs and the European Union to build a new cable stretching from Spain to Brazil in order to circumvent transferring data through the United States. If the United States decides to continue its current cyber policies, the alternative cable would limit the amount of data the U.S. could intercept within its physical borders.

As part of a continued effort to move off U.S. based software and hardware, Brazil is also moving off of Microsoft Outlook for its email services.[190] Instead, the Brazilian government will use an already developed Linux alternative.

President Rousseff is not the only foreign leader working against the United States as a result of being targeted by U.S. cyber efforts. German Chancellor, Angela Merkel, shared sharp words against the United States after documents revealed her phone had also been tapped by the United States, this time working in conjunction with Britain's MI6. Chancellor Merkel announced plans in February, 2014 to help build a secure communications network within Europe in order to circumvent U.S. spying efforts.[191]

---

[189] Mari, Angelica. 2014. "Brazil Passes Groundbreaking Internet Governance Bill." *ZDNet*. March 2. http://www.zdnet.com/brazil-passes-groundbreaking-internet-governance-bill-7000027740/.

[190] Miller, Claire Cain. 2014. "Revelations of N.S.A. Spying Cost U.S. Tech Companies." *The New York Times*, March 21. http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

[191] Paterson, Tony. 2014. "Surveillance Revelations: Angela Merkel Proposes European Network to Beat NSA and GCHQ Spying." *The Independent*. Accessed April 21. http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html.

Additionally, the European Parliament called on the European Commission to "suspend the safe harbor data privacy agreement with the U.S."[192] The US-EU Safe Harbor agreement is an option for U.S. companies to more easily comply with the EU Data Protection Directive. The directive guarantees European companies work to protect accidental leaks of personal data. Suspending the agreement would stop U.S. companies that do not comply with the EU Directive from being able to operate in Europe thereby impacting potential profits. The European Commission has opted to maintain the agreement and has instead offered possible reforms for the United States.

The German government has also announced plans to ramp up its own counter espionage efforts, highlighting the United States as the main antagonizer and relocating efforts away from Russia, China, and North Korea.[193] Besides the initial effects of having U.S. allies more suspicious and untrustworthy of U.S. activities, the effect of distracting ongoing efforts away from investigating our strategic threats is a significant waste of resources.

Technology companies such as Facebook, Google, Apple, Yahoo, and Microsoft have been widespread recipients of blowback and have subsequently pressured the U.S. for reform. In 2013, the FBI requested the access codes to Lavabit's email servers. Snowden used Lavabit in order to send encrypted emails. Instead of giving up the master key, Lavabit chose to shutdown.[194]

The leaks revealed that the NSA or FBI had pressured Microsoft to make Skype less secure and more susceptible to spying. Instead of shutting down as Lavabit had done, Microsoft made the necessary change in order to make eavesdropping easier for government forces.

Besides backlash from overseas, the revelations have similarly caused widespread domestic responses. Many Americans have interpreted the leaks to imply that every American citizen is being

---

[192] Baker, Jennifer. 2013. "EU Will Not Suspend Safe Harbor Data Privacy Agreement with the US." *PCWorld*. November 27. http://www.pcworld.com/article/2067480/eu-will-not-suspend-safe-harbor-data-privacy-agreement-with-the-us.html.
[193] Paterson, Tony. 2014. "Surveillance Revelations: Angela Merkel Proposes European Network to Beat NSA and GCHQ Spying." *The Independent*. Accessed April 21. http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html.
[194] Levison, Ladar. 2013. "Lavabit." *Lavabit*. http://lavabit.com.

watched and investigated by the NSA. Even a former President of the United States believed his email is being monitored. Former President, Jimmy Carter, explained his concerns in a recent interview with NBC's Andrea Mitchell saying, ""You know, I have felt that my own communications are probably monitored…And when I want to communicate with a foreign leader privately, I type or write a letter myself, put it in the post office and mail it."[195] The probability of Mr. Carter's communications being monitored is exceedingly low; nonetheless, Mr. Carter's sentiments reflect the growing sentiments of average citizens over concern for abuse of power.

General Keith Alexander has since announced that Mr. Carter can return to writing his emails because he is not being monitored.[196] An additional source of backlash stems from the NSA's incorporation of vulnerabilities in secure software. When it comes to creating safe and secure computer systems, using a tested encryption method is key to maintaining a high level of protection. Encryption methods are not all equal. The encryption methods that the military use are undoubtedly stronger than those used by the average citizen.

Thus, when the Snowden revelations exposed the intentional flaw in encryption design to create a vulnerable system for the NSA, the ramifications echoed through the tech world. Snowden documents affirmed that security company RSA Security was paid $10 million by the NSA in order to install a backdoor into its encryption methods.[197] The backdoor allows for the NSA to more easily break the encryption methods Extended Random and Dual Elliptic Curve.

The ability to break into encryption is a pretty powerful step for the NSA. However, losing that ability will flex, not break the NSA's abilities. The weakness of every encryption method is similar to that of a network. Given enough time and computing power it is possible to break into any encrypted

---

[195] Stableford, Dylan. "Jimmy Carter Believes U.S. Is Spying on Him." *Yahoo News*. http://news.yahoo.com/jimmy-carter-nsa-spying-164434808.html.

[196] Alman, Ashley. 2014. "Keith Alexander: NSA Isn't Spying On Jimmy Carter's Emails, So He Can Stop Using Snail Mail." *Huffington Post*. March 25. http://www.huffingtonpost.com/2014/03/25/keith-alexander-jimmy-carter_n_5031701.html.

[197] Menn, Joseph. 2014. "Exclusive: NSA Infiltrated RSA Security More Deeply than Thought - Study." *Reuters*, March 31. http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331.

document. The NSA's new facility in Utah is a powerhouse of computing power that can be concentrated to break virtually all common encryption methods.

The United States should expect that tech-savvy individuals will seek to create an even more secure encryption method in order to thwart intercepting efforts. As of March 2014 Google now offers encrypted searches by default in China and will likely make that standard globally.[198] [199] Google also introduced encrypted transfer of emails between servers making intercepting emails significantly more difficult and time consuming.[200]

We should expect in the coming months for stronger encryption technologies to be introduced, especially from the open-source community as their code is able to be peer-reviewed. Several new encrypted text messaging services has been created since the leaks began. While the average American is not being monitored, the overall increase in encrypted packets will obfuscate data that is actually valuable to the intelligence community.

Enhanced encryption methods will also deter the ascertainment of critical intelligence for monitoring. The impact of this loss in intelligence will undoubtedly increase the working time necessary to gain, crack, and analyze data packets and thereby decrease the ability of the intelligence community to review that data.

Part II - The Response from the United States.

The United States, specifically the NSA, has responded to allegations of data theft, posing as Facebook servers, and spying on Americans and non-Americans by offering half-truths and partial apologies.

---

[198] https://encrypted.google.com/

[199] Timberg, Craig, and Jia Lynn Yang. 2014. "Google Is Encrypting Search Globally. That's Bad for the NSA and China's Censors." *Washington Post*. http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/google-is-encrypting-search-worldwide-thats-bad-for-the-nsa-and-china/.

[200] Wilhelm, Alex. 2014. "Gmail Traffic Between Google Servers Now Encrypted To Thwart NSA Snooping." *TechCrunch*. http://techcrunch.com/2014/03/20/gmail-traffic-between-google-servers-now-encrypted-to-thwart-nsa-snooping/.

The most famous NSA response came from the Director of National Intelligence, James Clapper. Clapper was called to testify before a congressional committee on March 12, 2013 to address concerns that the NSA had been bulk-collecting data of American citizens. When directly asked by Senator Wyden if the NSA collects any type of data at all on Americans, Clapper confirmed that the NSA does not "wittingly" collect any such data.[201] Soon after the hearing, several more files revealed that the NSA does, in fact, collect widespread meta-data on U.S. citizens.

In an interview in June, Clapper explained his earlier denial of bulk-collection saying, "I responded in what I thought was the most truthful, or least untruthful, manner by saying 'no'."[202] Unfortunately, that kind of response did not satisfy the American public and led to widespread uproar of NSA activities.

In March of 2014, former director of the NSA, Micahel Hayden, gave an interview with a German new site, Spiegel Online. During the interview, Hayden said he was prepared to apologize not for the NSA spying on an ally, but rather for the awkward position this put the ally in.[203] His statements both reflect the sentiment that the United States does not have to answer for its activities and the self-assuredness that the activities are legally valid.

President Obama announced a plan at the end of March, 2014 to reform the legality of NSA data collection. However, the reform falls short of the true change to the program and has thus far not been received well by the public. Take for example, Michael Brenner, longtime writer for the Huffington Post and Senior Fellow for the Center of Transatlantic Relations, described the NSA reforms using extremely colorful language arguing, "We have created a monster. A Great White Whale that rapaciously stalks the

---

[201] *Director of National Intelligence James Clapper Indisputably Lied to Congress About NSA Surveillance*. 2013. http://www.youtube.com/watch?v=4v7YtTnon90&feature=youtube_gdata_player.

[202] Reilly, Mollie. 2013. "James Clapper: I Gave 'Least Untruthful' Answer Possible On NSA Surveillance (VIDEO)." *Huffington Post*. June 11. http://www.huffingtonpost.com/2013/06/11/james-clapper-nsa-surveillance_n_3424620.html.

[203] Hujer, Interview Conducted By Marc, and Holger Stark. 2014. "SPIEGEL Interview with Former NSA Director Michael Hayden." *Spiegel Online*, March 24. http://www.spiegel.de/international/world/spiegel-interview-with-former-nsa-director-michael-hayden-a-960389.html.

electronic seas devouring all within reach regardless of species or nutritional value."[204] Brenner's frustration echoes that of the average citizen, unable to trust the forces that were created in order to protect us.

Brenner highlights two major facts that discredit the reform. First, the legislation does not introduce any changes to collection of digital communications and instead chooses to focus almost exclusively on phone meta-data collection. Second, since the rest of the Five Eyes are not subject to similar oversight they can still collect the necessary data to which the NSA can then access. Introducing only partial reforms will not quell the rising distrust and dissatisfaction within the American public.

Part III - Suggestions for Moving Forward

The U.S. has largely been pummeled by the continued leaks and lost the trust of the American citizens. Bruce Schneier, a cryptology expert and widely revered writer, explains in a July 2013 blog post the necessity of trust saying, "Trust is essential in our society. And if we can't trust either our government or the corporations that have intimate access into so much of our lives, society suffers. Study after study demonstrates the value of living in a high-trust society and the costs of living in a low-trust one."[205] Moving forward, it is paramount for the NSA and corresponding government agencies to restore the trust of its people.

The major issue is that dozens of states conduct various degrees of cyber espionage and by focusing solely on the U.S.' activities then other states are allowed to continue their activities without the same level of scrutiny. If the United States stands alone under the microscope, then it will lose its strategic advantage as a cyber power because other states will learn how to defend against possible attacks. Now that the pressure is on the Western countries, equal attention should be given to the Eastern states also engaged in all forms of cyber espionage and cyber operations in order to give equal balance to the issue.

If the United States were to stop each one of its activities as they came to light, the U.S. would be in an extremely vulnerable position militarily and economically. In theory, the programs are set up to

[204] http://www.huffingtonpost.com/michael-brenner/obamas-nsa-reform-another_b_5063077.html
[205] Schneier, https://www.schneier.com/essay-435.html.

protect Americans from all kinds of attacks. Instead, balance should be restored so as to restore focus not only on the United States' activities, but also on the activities of Russia and China.

Additionally, the United States, specifically the NSA, should act to stop the leaks and ongoing revelations by getting ahead of the leakers. One of the reasons the Snowden leaks have been so impactful is that the reporters releasing the files have been very successful in keeping the public entertained. By slowly releasing the files it is like following a chronicle and each new story fuels the public drive for more. Working in conjunction with the slow leak, when U.S. officials either outright refuse the program exists and are then proven wrong, or refuse to comment on the supposed program, the U.S. losses significant political influence.

Another major issue is the blending of wartime activities in peacetime. Listening to phone calls, intercepting emails and texts, and monitoring the metadata of cell phones appear very much in line with the activities of a country at war. Now we are finding that the activities of the U.S. government very much mirror the activities of our supposed adversaries like China and Russia. In the fight for ideological imperatives, the more similar to we are to the enemy the harder it is to distinguish ourselves from them.

One strategy to get ahead of the leaks is to completely reveal every program Snowden could possibly leak in conjunction with solutions to suspected oversight issues. This strategy would leave the United States extremely vulnerable to International sanctions or pressure and is the least preferable method.

Another strategy is to redirect attention away from the United States by releasing information on other states' cyber programs. This strategy brings the issue more into the international field but also side-steps the major domestic issues. Drawing attention exclusively to the U.S. ignores the larger issue that virtually every state with a cyber initiative carries out similar data-collection programs. Simply because the United States is carrying out the program the best does not exclude the other states from undergoing the same level of scrutiny.

If the U.S. were to spearhead this effort then it should expect setbacks. The optimal way to accomplish this task is to instead work through non-states in order to leak the information. Sites like Wikileaks are ideal means to publish such information if this tactic is used.

When the United States' actions are taken into consideration in the broader global context, their actions become fairly reasonable for protecting American citizens. In the 2008 attacks on Mumbai, the terrorist group Lashkar-e-Taiba used Skype to coordinate between on the ground troops and handlers.[206] Through Google Earth, Twitter, and the news, the brains behind the attacks could help navigate the on the ground troops in order to maneuver around the police. If the United States wants to prevent similar scenarios from occurring within its borders, then having control of Internet communication is key to preventing the attacks.

The trick will be to balance the seeming invasion of privacy with the need for protection. I believe opening the process up for review by key figures in both the technological world and military system will help build a balance of opinions. Becoming too transparent opens up the possibility of compromising the security of the projects. If the technology corporations, in conjunction with some international input, could elect a few appropriate representatives then the process could begin for rebuilding the trust the American populace desperately desires.

In conclusion, the United States has taken huge hits as a result of the ongoing leaks, but there are still options available to help prevent more hemorrhaging blowback. Relations with other countries can be repaired through diplomatic openness and shared research projects that benefit the interests of both countries. Rebuilding the trust between the U.S. will help the United States secure its borders as more allies will be willing to share information. The United States would also benefit by better framing its cyber activities instead of allowing the leaks to dictate the conversation. Purely reacting to exposes ultimately keeps the topic in the public conversation longer than a move to get ahead of the leaks.

---

[206] Allen, Ian. 2009. "Comment: EU Wants to Intercept Encrypted VOIP Communications." *intelNews.org*. http://intelnews.org/2009/02/25/01-85/.

Now that I have entailed the numerous aspects of cyber conflicts, I will move into an assessment for how various activities can be improved.

CHAPTER 8: RECOMMENDATIONS FOR IMPROVEMENTS TO CYBER INFRASTRUCTURE AND OPERATIONS

"I know somebody's coming. At some point, somebody's coming at me. It's going to happen." -Scott Saunders, Information Security Officer for the Sacramento Municipal Utility District in California.

The cyber world is created from thousands upon thousands of servers and cables that traverse the world. Every point is a potential vulnerability able to be exploited by enemies. In this chapter, I will bring together the research from dozens of advisory groups to make a unified recommendation about how the United States can improve the security of its cyber infrastructure.

Every President of the United States since the 1980s has warned that U.S. cyber infrastructure is vulnerable to attack and called for immediate improvements to be made.[207] To this day, cyber threats are unequivocally named the top threats to national security. Speaking in 2013, "James Clapper, the director of US National Security, said cybersecurity is "first among threats facing America today,"[208]. Yet, for all the talk of cyber security, the United States has been depressingly slow in its efforts to pursue a more defensive cyber infrastructure.

One

My first recommendation is to phase out the use of commercial software from government cyber infrastructure. I realize this is a pretty monumental task seeing as the United States lacks the capacity to completely develop its own software, but if implemented over a long period of time the United States could become substantially more secure against a cyber attack.

Microsoft's Windows XP was created in 2001 and heralded as the operating system of a generation. Yet that generation is quickly ending and the United States is not making changes to protect itself. Twice now Microsoft has announced that it will no longer be releasing updates for the now outdated Windows XP and been forced to create an expanded timeline for phasing out the OS.

---

[207] Brenner, Joel. 2011. *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press. Pg 233.
[208] "New Cyber-Attack Model Helps Hackers Time the next Stuxnet." 2014. *The Conversation*. January 13. http://theconversation.com/new-cyber-attack-model-helps-hackers-time-the-next-stuxnet-21985.

Additionally, commercial software is built to do a variety of tasks, many of which government offices do not take actively use. Eliminating the extraneous capabilities also serves to remove possible points of exploitation. The U.S. Navy figured this out and has begun building its newer warships completely run by Linux – open source computer code. The U.S.S. Zumwalt will be the first of its kind to be completely operated by a variety of Linux based operating systems. The warship's software does not contain extraneous code unnecessary to the operation of the ship.

Moving away from commercial software is a contentious move because it would essentially require the creation of a government software department that has coders available to help with every other department. There are some obvious concerns with the U.S. government being responsible for their own IT infrastructure, especially after the blundered roll out of the Affordable Care Act Website. However, if top programmers were offered competitive salaries then it is theoretically possible for the government to run a successful in-house I.T. Department.

Furthermore, the United States would have access to the source code and could make changes when necessary, instead of relying on a commercial vendor to release security patches. Microsoft is not keen on releasing the underlying code behind its commercial software.

The software could also be custom designed to have modular components. Each computer terminal would run on a core piece of software that could then have pieces activated by necessity. Having a modular system would disable unnecessary code being active on a department's account, thereby reducing the level of security risks potentially active in any one computer. Just like the USS Zumwalt is custom built for specific tasks, each department's computers would then be customized to remove unnecessary capabilities, thereby mitigating potential software vulnerabilities.

Within the realm of cyber warfare, having a custom built system makes the entry into attacking U.S. Government systems significantly hire. Microsofts' software is the largest target of cyber attacks for multiple reasons, the two most significant being A) the widespread implementation of Windows flavors and B) the relative vulnerability of the code. Cyber attackers can learn the vulnerabilities on one operating

system and then attack both public and private companies around the globe. If the United States had its own system then it would essentially isolate itself from a large quantity of attacks.

A custom built system would also significantly increase security by raising the cost of an attack. In the case of Stuxnet, the United States spent millions of dollars building an identical system to the Natanz enrichment facility for vulnerability testing. As detailed in the 2011 National Military Strategy, one of the highlighted concerns was the low barrier to entry in launching a cyber attack.[209] With a custom built operating system, non-state actors seeking to attack the United States would have a much harder time carrying out an attack against the United States because of the sheer amount of resources necessary to conduct such an attack. The non-state actors would need to A) Get hold of the protected operating system B) Be able to decrypt it (harder than it sounds) C) Review the entire source code for vulnerabilities D)

Moreover, the software could be configured to be isolated to a specific network if a serious intrusion is detected. In the case of another Titan Rain scenario, the United States could activate the kill switch to severe all computers' ties to the outside Internet, thereby stopping the leak. As in the case of Russia's invasion into Estonia, virtually all communication between government departments was ground to a halt when the cables carrying the Internet traffic were completely inundated with senseless traffic. With a custom build operating system working in conjunction with the private bodies that control the flow of Internet traffic, government communications could continue as normal to facilitate a collective response.

Two

The second recommendation is for the United States to follow the same standard set by its European counterparts by incorporating more consumer protection against credit card theft. This change would help reduce potential loss from credit card thefts and ultimately reduce cases of cyber espionage.

[209] Mullen, M. G. 2011. "The National Military Strategy of The United States of America". Government Report. Washington, D.C. http://www.army.mil/info/references/docs/NMS%20FEB%202011.pdf.

The United States experiences the highest percentage of credit card abuse with an average of 44% of cardholders subject to fraud.[210]

Implementing Europay, MasterCard, and Visa (EMV) standards would help to mitigate potential credit card thefts through increased technological security. Most credit cards in the United States use a magnetic strip and signature in order to make purchases. The EMV standard improves security by using a PIN, much akin to transactions completed via a debit card, and an imbedded chip to identify the card. American banks are currently transitioning to the EMV standard, but the transition is slow because all the technology for reading cards has to be physically replaced.

Three

The third recommendation is to actively seek out and employ non-state hackers to work for the government. It is unclear if the United States does not already do this, therefore I have included it in the recommendations. As discussed in chapter two, China actively holds competitions in order to recruit civilian hackers for the government. There are hundreds of hack-a-thons in the United States but the events lack the same emphasis of ultimately joining the state that the Chinese have embedded into their events. The emphasis is instead of joining major companies like Google, Apple, or Microsoft instead of joining cyber defense.

Additionally, the Snowden revelations have hurt the image associated with working for the United States cyber forces, leading to a stigma placed on those that work for the NSA or CIA. The civilian military forces must regain the trust of the American citizen in order to recruit more qualified candidates to defend U.S. interests.

Four

One of the single most frequently called for changes that needs to be made is for the United States cyber forces to all communicate with each other.[211] I would be remiss if I did not recommend the same.

---

[210] Touryalai, Halah. "Countries With The Most Card Fraud: U.S. And Mexico." *Forbes*. http://www.forbes.com/sites/halahtouryalai/2012/10/22/countries-with-the-most-card-fraud-u-s-and-mexico/.

In the 1990s, anti-virus groups used to work independently of each other to collect data on various malwares and independently create patches. However, the process of finding and collecting data on the pieces of malware created a major choke point in the turn around time for producing patches. The companies then elected to share databases in order to reduce the amount of time necessary to gather information and thereby increased the speed at which the companies could produce solutions.

The United States should learn from this example by similarly making their databases of known vulnerabilities open to each agency. As of currently, the federal and state agencies operate independently of each other to create these databases. Moving to a system in which agencies at all levels of government have access to the database would vastly increase the number of employees able to protect state sites against possible attacks.

There are some notable challenges in creating a shared database. Joining the databases then creates a legal dilemma between public and private interests. Private industry will then request access to the databases in order to create a more secure site. If the NSA wishes to continue using the exploits, exposing the vulnerabilities to private industry would vastly eliminate the number of available intrusion methods. I believe the gain of protecting U.S. companies from intrusion is greater than the relative loss of available exploits. Thus sharing the database with U.S. companies would be a positive step towards protecting U.S. companies from cyber intrusions.

Five

The United States needs better control over its relation with China. Chinese espionage continues to increase among virtually all sectors of the United States. The United States public and private sector has been aware of Chinese espionage efforts for at least the past 15 years, yet virtually every year new attacks penetrate U.S. defensive networks.

In 2003, Chinese government hackers conducted one of the most massive data breaches in U.S.

---

[211] "Fact Sheet: Executive Order on Cybersecurity / Presidential Policy Directive on Critical Infrastructure Security and Resilience." *Department of Homeland Security*. http://www.dhs.gov/news/2013/02/13/fact-sheet-executive-order-cybersecurity-presidential-policy-directive-critical.

history, titled Titan Rain. In 2007, the DoD and other government agencies "and defense-related think tanks and contractors experienced multiple computer network intrusions, many of which appeared to originate in the PRC."[212] The same year, Jonathan Evans, Director-General of he British intelligence service, "alerted 300 financial institution officials that they were the target of state-sponsored computer network exploitation from the PRC."[213] A 2013 summary of the Chinese military explains, "In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military."[214] These attacks occur despite President Obama's efforts to create transparent cyber activities with China.

Six

The United States leadership must to learn more about cyberspace in order to make informed decisions. Singer explains in a February interview, "Reportedly Obama has expressed his 'frustration that the complexity of the technology was overwhelming policymakers.'"[215] Policy makers must be experts on the subject for which they are writing laws. This policy is not necessarily a cyber-specific recommendation but simply embraces the totality of how policy should be correctly made. When governments treat cyber space as an extension of physical space and then create laws based on that assumption, they are ultimately creating bad policy and hurting Americans.

The U.S. Supreme Court is the ruling body on judicial issues, including issues related to the cyber world, such as the upcoming case on the legality of NSA spying. However, the Supreme Court as a whole lacks a basic grasp of rudimentary cyber tools. For example, the Supreme Court Justices do not use email

---

[212] "Annual Report to Congress: Military Power of the People's Republic of China 2008." 2008. Annual Report. Washington, D.C.: Office of the Secretary of Defense. http://www.defense.gov/pubs/pdfs/china_military_report_08.pdf.

[213] Ibid.

[214] "Annual Report to Congress: Military Power of the People's Republic of China 2013." 2013. Annual Report. Washington, D.C.: Office of the Secretary of Defense. http://www.defense.gov/pubs/2013_china_report_final.pdf. Pg 36.

[215] Roggeveen, Sam. 2014. "Interview: Peter Singer on Cybersecurity and Cyberwar." *The Interpreter*, February 4. http://www.lowyinterpreter.org/post.aspx?COLLCC=2495499624&COLLCC=2845155361&id=fd67a95a-a3a2-480a-bbd7-954c4e7fc958.

because they "[haven't] really gotten to [it]."[216] How can the Supreme Court be relied on to decide on complex issues related to cyberspace when they lack the elementary understanding of cyber tools?

As further proof of a widespread technological naiveté, Janet Napolitano, the Secretary of Homeland Security, admitted in a 2012 interview that she "just didn't believe e-mail useful."[217] These basic functions of cyberspace are being protected, infiltrated, and decided on by government employees that lack a fundamental understanding of cyberspace.

Seven

In its current structure, there are a number of issues that plague the cyber industry. First off, the fundamental change that needs to occur is the restructuring of the military infrastructure and policies surrounding cyber warfare. Infrastructure-wise, the United States has taken strong steps forward by restructuring its cyber military operations under the CYBERCOM in 2009 under President Obama. This is a step in the right direction as the change assists in the communal sharing of resources. However, the widespread use of defense contractors in order to build cyber attacks opens up too many disconnected points for the military to act as a unified collective. As discussed in the previous chapter, the speed with which cyber actors can launch attacks necessitates a military structure that can similarly respond in near light-speed. Having a multitude of working parts slows down the ability of a government agency to launch attacks.

Second, the policies governing responsibilities of various government agencies must adapt to reflect real world challenges. Currently, the United States military code separates departments responsible for intelligence operations from military operations.[218] Separating the two operations creates an artificial divide between two virtually inseparable tasks. The two specific titles in question are Title 10 and Title 50.

---

[216] Oremus, Will. 2013. "Elena Kagan Admits Supreme Court Justices Haven't Quite Figured Out Email Yet." *Slate*, August 20. http://www.slate.com/blogs/future_tense/2013/08/20/elena_kagan_supreme_court_justices_haven_t_gotten_to_email_use_paper_memos.html.

[217] Singer, Peter W.; Friedman, Allan (2013-11-16). Cybersecurity and Cyberwar: What Everyone Needs to Know (p. 5). Oxford University Press, USA. Kindle Edition.

[218] Clarke, Richard A., and Robert Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It*. Reprint edition. New York: Ecco. Pg 222.

Title 10 restricts military operations to the three branches of the armed forces. Title 50 restricts intelligence gathering to non-military forces such as the NSA and CIA. Title 10 and Title 50 laws work to unduly restrict the movements of the military figures that are responsible for reacting and launching attacks.

Fortunately for the United States' cyber efforts, the military has already begun restructuring the military and civilian forces to blur the line between the laws. CYBERCOM's use of both military and civilian forces is a great example of how the laws no longer apply to current military structure. Throughout the past decade, the NSA has launched several attacks that put it outside of an intelligence-gathering agency. In 2005, the NSA infected 100,000 computers with its highly sophisticated malware. The malware allows for remote monitoring of the computer. By all means if the same attack was carried out by another state against the U.S. then it would be seen as a true cyber attack.

Third, the United States should make a strong push away from private contractors. Private contractors are a temporary solution for a much larger symptom – the slow reaction time of the federal government. Whether that is because the federal government cannot pay a competitive rate to qualified candidates or because the federal government has too much oversight that the process for hiring employees is too slow – these are symptoms of a larger need for restructuring. Opening up the work to contractors similarly opens up vulnerabilities that play out in U.S. military capabilities. Singer discusses his experience with a mock cyber attack explaining:

> In one 2012 Pentagon-sponsored war game we participated in, a simulated enemy force hacked the contractor company supplying the logistics of a US force, with the simple purpose of transposing the barcodes on shipping containers. It seems a minor change with little impact. But had it been a real attack, US troops in the field would have opened up a shipping pallet expecting to find ammunition and instead only found toilet paper.[219]

War simulations should not be placed on the same level as real world experiences. Yet, the reason for the simulation is to learn and improve, thus the lessons should not be discarded as irrelevant. The 2012 Pentagon-sponsored simulation may have not have been a real occurrence, but it certainly demonstrates

[219] Singer, Peter W.; Friedman, Allan (2013-11-16). Cybersecurity and Cyberwar: What Everyone Needs to Know (p. 131). Oxford University Press, USA. Kindle Edition.

possible real world manifestations of an attack and points of entry for attackers. Those that wish to harm the United States will look beyond the U.S. military for viable targets. Contractors then become a source of vulnerability, as each one must be secured lest they become the entry point for an attack.

In conclusion, the road ahead for the United States is long and arduous. How the United States approaches the next decade will fundamentally decide its cyber influence extending well into the 21st century. In order to be successful the United States must adopt new, unprecedented policies and have the courage to stand behind those activities publicly. Non-state actors are on the rise and new technology aimed at completely shrouding the identities of cyber actors will only provide a more fertile environment for dissent in cyberspace. The United States cannot hope to control the ideological components of cyber actors the same way it has tried to extend its influence physically in the past. The issues discussed in this thesis require a fundamental restructuring of the thinking involved in cyber operations. Old war mentalities to try and understand the workings of non-state cyber actors have proven unproductive. I believe technology is moving in a direction in which central control of communication will no longer be a reality. Government attempts to monitor communications will prove wholly unrealistic and technically impossible. The United States could take a strong stance forward by relinquishing a portion of its power in order to regain its standing as the pioneer of freedom and liberty. Yet, history's most often repeated lesson is that those in power almost never voluntarily surrender it.