THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY

THE WAKE OF CYBER-WAREFARE

STUDENT NAME JACOB SISKO
SPRING 2015

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Security and Risk Analysis
with honors in Security and Risk Analysis

Reviewed and approved* by the following:

Gerald Santoro
Senior Lecturer Professor Information Sciences and Technology
Thesis Supervisor

Edward Glantz
Senior Lecturer Professor Information Sciences and Technology
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

The purpose of my thesis paper is to explain the significance and inter-relationship of cyber-crime and cyber-warfare. To give my reader a full understanding of the issue, I will begin by explaining the history of the Internet, give a definition of both cyber-crime and cyber-warfare, and then explain how they have impacted the Internet. I will also give examples of a few Chinese hacker groups, and what kind of attacks they have successfully carried out. Then I will talk about how recent attacks have become more sophisticated which are capable of causing more damage. I would also like to discuss how the cyber-warfare has impacted Chinese-US relations, and how it has an impact on the economic ties. Because of the currently capability and potential threat, I will explain why cyber-crime and cyber-warfare are so important to monitor because of the potential damage current and future attacks can cause.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to thank my honors advisor, Dr. Edward Glantz for helping me get on track for success. Most importantly I would like to thank Dr. Gerry Santoro, who spent hours of time with me to help guide and revise me along the process of producing my honors thesis. Without his help and support my thesis would be nonexistent. I would also like to thank Anna Squicciarini and my mom, Martha Sisko, who pushed me to keep going when it became tough for me and I was unsure if I was going to finish it.

Chapter 1

Introduction

Cyber-crime and cyber-warfare are emerging as significant threats in today's world. Cyber-warfare is "Internet-based conflict involving politically motivated attacks on information and information systems" whereas cyber-crime is "illegal activity that is done on a network or via the internet" (Searchsecurity). It is becoming an increasing problem because in a modern world where everything is becoming digital and controlled electronically, there is much more at stake. In order to fully grasp the potential danger of cyber-crime and cyber-warfare, it is important to understand the history of the Internet, early forms of cyber-crime, how cyber-warfare has emerged, examples of hacker groups and their methods, and based on the trends, the potential outlook of cyber-warfare in the future.

History of the Internet

Back in August 1962 J.C.R Licklider became the first head of computer research for DARPA (Defense Advanced Research Projects Agency), on a mission of creating a a network that could connect computers across the United States. Later one of his successors, Lawrence ran with the idea and established ARPAnet (Advanced Research Projects Agency Network). In the beginning, only a few computers were connected to ARPAnet, starting with UCLA and Stanford Research Institute (SRI), UC Santa Barbara, and University of Utah, expanding several others

(Cerf, Vint). ARPAnet was originally designed as a computer version of the "nuclear bomb shelter," which was the concept of building a network of computers that could withstand an nuclear bomb without losing any information. Once the number of users on ARPAnet increased so extensively, many of whom were non-military users, the military created its own, safe military network in 1983, called MILnet. Finally, in 1986, the National Science Foundation established a new network, called NSFnet, which eventually outperformed the slower network, ARPAnet, and became the backbone of today's Internet.

In 1989 Tim Berners-Lee, a software engineer at CERN, a large particle physics laboratory in Switzerland, developed the framework that would become the World Wide Web ("History of the Web"). Tim created three fundamental protocols that are still part of the foundation of the web today: HTML, URI, and HTTP ("History of the Web"). By the end of 1990 CERN had created the first web page ("History of the Web"). Because CERN wanted the web to grow, in April 1993 CERN announced that the World Wide Web would be available for anyone to use on a royalty-free basis. From then on, the Web has "changed the way we teach and learn, buy and sell, inform and are informed, agree and disagree, share and collaborate, meet and love, and tackle problems ranging from putting food on our tables to curing cancer"]. Because the Web became a public domain, many companies saw it as an opportunity to further conduct business and reach its consumers. By 1998, 750,000 commercial sites were on the World Wide Web where hotels, airlines and other industries were using the web to "further the power of the web as a sales medium" (Peter, Ian). As time progressed the World Wide Web has expanded tremendously, to facilitate business, leisure, and other daily activities. With the Internet spiraling upwards as it grew, it gave way to cyber-crime and cyber-warfare to exist over the Internet, but cyber-crime existed much earlier than the inception of the Internet.

Chapter 2

Cyber-crime – Functions and Capabilities

Although the web was not created until1989, cyber-crime emerged much earlier in computing history. Many early computer crimes consisted of physical damage to computer systems and subversion of the long-distance telephone networks (Kabay, M. E.). For example, in 1967 in Olympia, Washington, an intruder shot an IBM 1404 twice with his pistol (Kabay, M. E.). In another case in 1970 at the University of Wisconsin a bomb destroyed $16 million of stored computer data, killed one person and injured three more, while at New York University a few radical students place fire-bombs on top of Atomic Energy Commission computer in an attempt to free a jailed Black Panther (Kabay, M. E.). Other attempts to damage computer networks were seen at Wright Patterson Air Force Base in 1974 where four attempts to sabotage computers such as loosened wires, use magnets to erase data and put gouges in the equipment (Kabay, M. E.). As a preliminary precaution to protect computers, security cameras were put to use to catch the culprit, which worked in 1972 when a night shift operator was caught in Denver crashing fifty seven disk head crashes on B3500 computers (Kabay, M. E.). Other early computer crimes were inside jobs, where an employee would alter database or financial information of a company, often in an attempt to embezzle funds.

In time, various types of malware were designed to be capable of new attacks, and with the development of new technology, the malware was designed to exploit the new vulnerabilities. While early forms of malware were simple, and were not capable of causing damage, newer forms of malware are much more sophisticated.

Tools of Attack

The primary motives behind much of the cyber-crime of the 1960s and 70s was desire for system access, curiosity, and the sense of power attained from defeating security (White, Kelly). Throughout time as computers became more common, people developed malicious software, or malware, for various purposes. Generally Malware is designed to "damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts or networks" ("What Is the Difference"). The types of malware are not mutually exclusive but they do have certain factors that can help distinguish one type of malware from another.

Trojan

A Trojan is a type of malware that is named after the famous 'Trojan Horse' of ancient Greece. A Trojan is a malicious piece of code that is hidden in legitimate code such as a document or program. What makes a Trojan so difficult to detect is the fact that it is a small piece of code and it is hidden within the code that the user intended to use. By taking out some of the original code and adding the code for the Trojan, it can still be very difficult for antivirus software to detect the malware. When a user is tricked into downloading and running the infected program or file, the Trojan is activated and can perform a range of attacks. One popular attack is to install a 'back door' on the device so that the attacker can have user access in the future, but Trojans can also cause damage through actions such as deleting files or stealing data. Trojans can also simply irritate the user through actions such as changing the settings or popping up

windows. Unlike other malware, Trojans do not reproduce themselves or self-replicate, they must be spread through the user such as through email attachments ("What Is the Difference").

One notable Trojan horse was Zeus. The Trojan was discovered in January 2010 and in just over a month about 75,000 machines were compromised. The Trojan was spread through spam and drive-by downloads. Drive by downloads happen when a piece of code is downloaded onto a machine simply by visiting a web site, without knowledge of the user. Because of the drive-by download, users were falling victim to the malware without their knowledge. Zeus was designed to steal personal information such as bank account information, and within a year it enabled the cyber-criminals to steal approximately $70 million (Nahorney and Falliere).

Virus

A virus is a type of malware that "propagates by inserting a copy of itself and becoming part of another program" ("What Is the Difference"). Whereas a Trojan hides itself within the code, a virus is malicious code that is built into the original code, but it was not necessarily hidden, and it is programmed to spread itself, which allows it to infect other machines. A virus is typically found in an executable file, which is a file that is simply loaded into memory and run. When the executable file is run, the program will run its normal course but in the background the executable will run as well and may try to overwrite other software or documents with itself. A virus can be spread when the file or software it is attached two is shared with another computer on the network. The capacity of the virus can range from minor annoyances to actual damage to data or software ("What Is the Difference").

An example of an early virus is the Melissa virus, which was released in 1999. The Melissa virus was one of the first computer viruses to spread through email. Melissa was called a 'macro virus' because it was hidden in the macro area of Microsoft Word documents and executed when the document was loaded into Word. The virus was programmed to replicate itself and send itself out to the top 50 addresses in the victim's Microsoft Outlook address book, which would continue the same process on each computer. The Melissa virus caused about $1.1 billion worldwide. The Melissa virus was one of the first viruses to achieve "rock star" status because of how well known it was.

As time progressed and people learned what types of viruses were successful, they used the code to improve the malware and make it more sophisticated so that it is more damaging. It is evident that after the Melissa virus, the virus inspired other more costly attacks. For example, in 2000 Love bug was also a self-replicating virus sent through email in peoples in a users email address book. As opposed to the Melissa virus, Love Bug forwarded the email to all of the users' contacts rather than just the first fifty. Additionally, Love Bug was coded and designed to delete .jpg and .jpeg file and alter .mpg files so that they become corrupt. Furthermore, the purpose of the virus was to search the victim's hard drive in search of password files and send them to the account located in the Philippines. By the end of the attacks, Love Bug caused $10 billion of damage in about twenty countries (Ingram, Mike).

Worm

A worm is another type of malware that is similar to a virus because they "replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses,

which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate" ("What Is the Difference"). Worms exist as processes in the infected computer. A worm can penetrate into a system through a vulnerability or through the use of social engineering to convince a user into executing the worm. Once the worm is on the computer via the vulnerability, the worm would then take "advantage of file-transport or information-transport features on the system, allowing it to travel unaided" ("What Is the Difference").

A well-known early worm was the 'Morris worm', which was accidentally released in 1998. Robert Morris, a graduate student at Cornell University created the worm (Menninger, Marc). With only ninety-nine lines of C code, Morris was able to shut down almost ten percent if the world's servers ("Internet Timeline"). The destructive power of this worm was due to errors is the code, which allowed the worm to replicate at an amazing rate. By the time the worm was stopped over 6,000 computers were infected. The damage from the worm did not cause anyone to lose data, but the estimated cost of damage was about $15 million.

Rootkit

A rootkit "is an application (or set of applications), that hides its presence or presence of another application (virus, spyware, etc.) on the computer, using some of the lower layers of the operating system (API function redirection, using of undocumented OS functions, etc.), which makes them almost undetectable by common anti-malware software" ("What is a Rootkit"). First a rootkit requires a way to get onto the host's computer, and it can be done through a variety of ways such as through social engineering, password cracking, spear phishing, or a Trojan. Once

the rootkit is on the computer, the attacker can obtain root or Administrator access, which allows the attacker to have all privileges on the system. A rootkit is difficult to detect because it is located at such a low level in the computer. Additionally, the rootkit may be programmed to hide from the software that is trying to find it, or worse yet, once on root access, the attacker could modify the software that is supposed to detect the rootkit ("Rootkit").

An incident that went to court recently was in 2006 when Sony BMG settled a case because they installed rootkits on the company's CDs to restrict users from copying music on their computer. On all of the CDs there was a Digital Rights Management (DRM) program which limited the number of copies that could be made. The program also had a rootkit built into it, but the problem was it left many computers vulnerable to attacks from third parties and it resulted in a lot of damage to many customers' computers. It also interfered with legitimate uses of the user's CD drive. As a result, Sony paid forty-two American states a total of $5.75 million in settlements as well as up to $175 per customer who suffered damages from the rootkit on their computer.

The Dropper

A Dropper is a type of "malware whose purpose is to deliver an enclosed payload onto a destination host computer." The Trojan horse is meant to carry the malicious code with it and not get detected by the virus-scanning software. Although the Trojan is not an infected file itself, its task is to carry the code into the system and "drop" the virus. Therefore, the dropper is used in the beginning of an attack to breach a network and set up way for more malware to enter into the host computer. When the dropper is executed, its code is designed to load itself into the memory,

extract the malware, and input it into the file system (“Trojan Dropper”). One example of a dropper is the Ngrbot Dropper which was released on Oct 4, 2013. In this scenario, the Ngrbot was targeting Skype users, as well as other social networking websites as well. To begin the attacks, the dropper sends the file to the targeted users with the file disguised as the same Skype icon so that it convinces the user that nothing is out of the ordinary and the files is safe. Depending on the user’s computer settings, the users may be prompted with a screen that asks for permission to run the Skype looking executable file. If that is the case and the user clicks to open the file, then the first step of the attack is successful, but if the user recognized that the file is suspicious and clicks “cancel” then the attack is stopped. From there if the fake file is downloaded, and the malware determines the public IP address of the system which is sent back to the attacker to establish a connection for further malware to be sent. Next the infected host sends infected messages to all of the contacts on Skype to attempt to infect their computers as well. After the computer system is infected, the malware can download and install other malware, which will be used to steal usernames, passwords and other information (“SonicALERT”).

Bot

A bot, short for robot, is “a program that operates as an agent for a user or another program or simulates a human activity” (“Bot (robot) Definition”). Bots can be used for good activity such as for “web crawlers… instant messaging (IM), Internet relay chat (IRC), or other web interfaces… [or for malicious activity such as] log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch denial of service (DoS) attacks [which

will be explained later] relay spam, and open back doors on the infected host" ("What Is the Difference"). A web crawler is an "internet bot that systematically browses the World Wide Web, typically for the purpose of web indexing" which is a way to organize the internet and may use metadata and keywords. When a bot is used for a negative purpose, it is because an attacker compromised a computer or other device to allow the attacker to control the compromised device in the future. Although the machine of a bot has been compromised, "bots rarely announce their presence with high scan rates… instead they infect networks in a way that escapes immediate notice" ("What Is the Difference"). The advantage bots have over worms is that bots have an even more versatile infection vector, and when a new exploit is published, the bots can be modified remotely so that they are still not detected ("What Is the Difference").

Methods of Attack

While Trojans, viruses, worms, rootkits droppers, and bots are different types of tools of attack that someone could use, there are also some methods of attack that are another way of causing a disruption to normal activity. Two common methods of attack are a denial of service (DoS) and a distributed denial of service (DDoS).

Social Engineering

An important method of attack that is sometimes overlooked is social engineering. Since the weakest link in computer security, it is a common method of attack used to gain access or steal information. Social engineering is "the art of manipulating people so they give up confidential information" (Criddle, Linda). Some common social engineering attacks include an

email from a friend that may contain a link or download that contain malware that will infect the computer, a phishing attack, baiting scenarios and more. A phishing attack is when an email or other message is sent and "appears to come from a legitimate, popular company, bank, school, or institution" in an effort to trick the user into sharing confidential information (Criddle, Linda). Although there are not many security practices to combat social engineering, two of best defensive practices are to be educated or informed of the types of attacks that are prevalent, and to not carelessly click on links simply because of curiosity.

Denial of Service (DoS) Attacks

A denial of service attack is a method of attack with the goal of prohibiting a user or set of users from accessing a desire resource. It is an attack that is "designed to bring a network to its knees by flooding it with useless traffic" (Beal, Vangie). Two common types of DoS attacks are the Teardrop attack and the Ping of Death. This works by flooding the Internet connection of the target site with millions of packets, many just simple pings. The flood sends large numbers of packets at a single network entry point, flooding the network, and denying legitimate packets to go through, effectively blocks legitimate traffic and makes the site unusable. Since a DoS attack originates from one source with the same Internet protocol (IP) address, it is easy for a computer network to block the one incoming source.

Distributed Denial of Service (DDoS) Attacks

Unlike a DoS attack, a DDoS attack comes from many computers simultaneously there by making it much harder to cut off the source. The DDoS attack is a method of attack that can

be carried out using a botnet (which will be covered later). It is a sophisticated and common attack that is frequently used by cyber-criminals. A denial of service attack is when a target, such as a website, receives an overload of network traffic in a condensed period of time, overloading the server. The excessive requests can cause normal users to be cut off from access to the website because the server is flooded with too many requests. Usually when such an attack occurs, the website owner will take the website offline to avoid having the hackers further attack the network while it is being flooded, or the website will crash by itself. A distributed denial of service attack is a collective attack that occurs from multiple machines, rather than from just one computer. Because it is easier and more effective to use more computers to complete a denial of service attack, a DDoS attack is usually performed, and it can be easily done with the help of a botnet.

DDoS attacks are very effective because they can thwart a target by taking them offline or prohibiting them from completing a task. DDoS attacks can be done to further a political mission or to simply carry out an attack. An example of how a DDoS attack can be used as a political statement was when Russia hackers attacked Estonia in 2007 with a DDoS attack. The reason for the attack was because Estonian nationalists wanted to move The Bronze Soldier, which was a symbol of when the Red Army soldiers "freed" the city of Tallin from Hitlar's control during World War II. The Estonians did not like the soldier because to them it reminded them of when Russia forced Estonian men to enlist in WWII, where seventy percent of the men died, when Russia forced 20,000 Estonian families to deport to Siberia in 1949, and when their deportation left them with no alternative but collective farming to survive. Because many Estonians were appalled by the statue, they decided to remove the statue from the center of the city to a remote cemetery ("Estonia vs. Russia: The DDOS War"). Vladimir Putin, although he

has publically criticized Estonia for defecting from the Soviet Union, is believed to have ordered the attack on Estonia, especially since "Estonian authorities claim that the attacks originate within Russia, and come from Russian government IP addresses" (Anderson, Nate). is a small country with about 1.3 million citizens, only a small government website server is needed to withstand the 1,000 visits per day. When Russian hackers launched the DDoS attack the server was received about 2,000 requests per second ("Estonia vs. Russia: The DDOS War"). Although there are not direct traces from Putin to order such an attack against Estonia, the timing of the attacks matched up with the time when the Estonian nationalists removed The Bronze Statue from the center of the city, making it seem as though it was a political message sent by Russian nationalists. According to an interview with Gadi Evron, who is a world expert on botnets and runs Israel's Computer Emergency Readiness Team (CERT), and helped resolve Estonia's problem, some of the traffic came from botnets that were purchased, and many of the attacks came from home requests from users that were attacking the websites manually ("Estonia vs. Russia: The DDOS War"). The first attack came on April 26th, and the attacks continued on and off for three weeks until May19th. During that three week period about 128 unique DDoS attacks were recorded to have been targeted at Estonia's infrastructure. The most DDoS attacks occurred on May 9th with fifty eight distinct attacks. Of the 128 DDoS attacks, seventeen of them lasted less than a minute while seven of them lasted ten hours or longer. Because of the capacity of the attacks, Estonia suffered serious down time of being offline, which affected its citizens because the attacks shut down government, banking, university and newspaper websites which hindered business and daily activities for a few weeks. One bank that reported its damages due to the DDoS attacks were about one million dollars and the attacks shut down credit card and ATM transactions for several days ("Denial-of-Service").

Chapter 3

Advanced Persistent Threats (APTs)

Another modern, sophisticated cyber-attack is an advanced persistent threat (APT). An APT is a "set of stealthy and continuous hacking processes often orchestrated by human targeting a specific entity, [which] usually targets organizations and or nations for business or political motives, [and] require a high degree of covertness over a long period of time" (Musa, Sam). An APT is not intended to cause damage or disruption to a system as other attacks do, the goal is often espionage. The top sectors that are targeted in APT attacks are government agencies, professional services (engineering, accounting, legal and health services), and non-traditional services (business, amusement, and repair-related services) ("Internet Threat Report 2014"). Similar in some ways to other modern methods of attack, an APT uses five phases to "break into a network, avoid detection, and harvest valuable information over the long term" ("Advanced Persistent Threats: How They Work").

The first of five phases of an APT attack is the reconnaissance phase, which involves surveying the target to understand how it operates. During the reconnaissance phase, the APT is prodding around on the network to try to look for vulnerabilities, weaknesses, and any other possible method to breach the network without being detected. The reconnaissance phase also included understanding what kind of hardware the target is using, the operating system that it runs, the version of the operating system and other applications, as well as the patches that have or have not been installed.

The second phase of the APT attack is the incursion phase, which is where social engineering is used to deliver the malware to take advantage of the vulnerabilities ("Advanced Persistent Threats: How They Work"). Since people are the most vulnerable target in an information system, social engineering is a useful skill that can easily allow an attacker to gain access to the target system. If social engineering is not used, other methods such as spear phishing are a viable option to breach the system. By using spear phishing, the attacker can trick the victim into clicking on a link, opening an infected message, or scare the user into sharing personal information, which will allow the attacker to breach the system.

The third phase of the APT attack is discovery. Once the attacker has infiltrated the network, the attacker stays low to avoid detection. The organization's defense is mapped and an attack is planned that will have multiple parallel kill chains ("Advanced Persistent Threats: How They Work"). Discovery is an important phase for an attacker because once the access has been gained the attacker will have the opportunity for other doors to open to gain access to other data and valuable resources on the network. In other words if one victim's computer on the network has been compromised, the attacker may have the potential to search other computers on the network for information that can be accessed from the infected computer.

The fourth phase of the APT attack is to capture data over an extended period. During the capture phase, other malware may be installed on the victim to be used to steal information. Once the valuable information has been identified, the attacker will gather the data together before it is exfiltrated. The capture phase has no set limit on how long it should take. Ideally the attacker wants to always remain unnoticed so that it can continually monitor and steal data from the victim.

The fifth phase and final phase of the APT attack is the exfiltration phase where the attacker has its malware send the stolen information back to the attacker for analysis, fraud, or other purposes. One process to exfiltrate the data may be done by uploading it to a remote server or website for the attack to see at any time. Another method of exfiltrating the data could be through encryption or steganography techniques in which the data is hidden inside DNS request packets so that the victim does not realize the information is being stolen ("Internet Threat Report 2014"). Although the APT attacks are laid out in five progressive steps, the order of the steps is not always followed. For example, once attacker has a foothold within a network, the last three phases may keep being repetitive. If the malware is stealthy enough to hide from the victim's knowledge, the attacker may continue to get new information as it becomes found, developed, or available over time. As the target is developed more information about its topic, the APT may continue to steal the new information that is being developed as well.

Chapter 4

Botnets

Another sophisticated attack is an attack performed by a botnet, or robot network. Botnets are made up of an army of bots, to attack a specific target. Bots can take over computers in a variety of ways, but the key is to do so undetected. A computer becomes a bot when a computer sends malware to another computer and exploits a vulnerability to take control of the computer. Once a computer has been taken captive as a bot, a message is sent to the master computer to let the computer know that it has control over the infected computer. Once infected, the bot sends the malware to other computer on the network to keep trying to capture more computers creating a botnet.

The bots can send a range of malware including spam, viruses, and spyware in order to gain control of a host. The bots will usually remain idle for a period of time, while the botnet is growing until the moment that the malicious user chooses to launch an attack. When the malicious user decides to activate the botnet, the user can tell each of the bots what to do, and the infected computers will suddenly respond and obey the commands sent out from the master computer ("Bots and Botnets—A Growing Threat"). Once the botnet has been acquired, botnets can perform a range of activities and attacks as directed by the master computer. One of the capabilities of a botnet includes the use of a "spambot" which sends spam emails to users. Other capabilities are to perform distributed denial-of-service (DDoS) attacks on a target, send ads to the infected users' computer in the botnet, or steal information from the computers once it is infected, such as credit card numbers, passwords, personal information, which is sent back to the malicious user. Botnets can also be used as an Internet proxy server for cyber-crime, as processing power to find Bitcoins to steal digital currency, and many other attacks (G, Tim).

Sometimes the malicious user, may not decide to launch an attack, but actually sell the botnet or a subset to a user who is interested in carrying out an attack of his or herself. Similar to how other online services can sell their products, a bot master can sell or rent out a botnet for someone else to use. Unfortunately, that allows users who are not tech savvy to be able to use a strengthened botnet for personal use by simply paying to the service. Symantec explains that a botnet large enough to bring down a website with a DDoS attack would only cost between $100 - $200 per day. Depending on the desired bandwidth, a more passive attack, such as a spambot or proxy could be rented for as little as $500 per month (G, Tim).

An example of a botnet that was used for an attack is the Chameleon botnet, which was released in 2013. The botnet has infected about 120,000 U.S. computers and was making a revenue of about $6 million per month due to click fraud on over 200 websites. The botnet is designed to scam web advertisers who have to pay about $0.69 per one thousand clicks on their advertisement. Of the 14 billion clicks that accumulated over time, 9 billion were credited to the botnet that is designed to make the advertisers pay for illegitimate clicks to the advertisement. The Chameleon is just one of many attacks that have been carried out through the use of a botnet (Kirk, Jeremy).

Chapter 5

Stuxnet

Stuxnet was an advanced cyber-weapon that was released in June 2009, and a lot of evidence suggests that the complex piece of malware was a state-sponsored attack from the United States and Israel against Iran (By state-sponsored I am referring to an attack funded and supported by a country/nation). Whereas the code to most malware is between ten to fifteen kilobytes, Stuxnet was "an extensive configuration file" of 500 kilobytes "with a menu of more than 400 items the attackers could tweak to control every aspect of the code, such as how long it should spread, and how long each exploit should work" (Zetter, Kim). In 2009 Iran was creating plans to increase and build its nuclear enrichment capabilities. In order to do so the Iranian government, led by President Mahmoud Ahmadinejad, installed about 8,700 centrifuges in a Natanz, a nuclear enrichment plant. Because of the capability of the source code, Stuxnet successfully damaged between 1,000 and 2,000 centrifuges, which needed to be replaced, in just a few months. As a reference, it is normal for about ten percent, or 870, of the centrifuges be replaced in a year, but for 1,000 to 2,000 centrifuges to be replaced in a few months was evidence that there was a bigger problem. Stuxnet "would come to be known as the most complex malware ever written… and would ultimately make history as the world's first real cyber-weapon" (Zetter, Kim).

Even though Iran's nuclear facility was an air-gapped Internet environment, meaning that the Internet was not accessible from the outside, the code to Stuxnet was able to penetrate into the facility because the code itself contained four zero-day exploits which strengthened the

ability of the attack. Zero-days are the "hacking world's most potent weapons: They exploit vulnerabilities in software that are yet unknown to the software maker or antivirus vendors" (Zetter, Kim). To express how rare a zero day is, anti-virus researchers find over twelve million pieces malware per year, and less than a dozen of them contain a zero-day. The first zero-day was a vulnerability in the LNK file of Microsoft Windows (Zetter, Kim), which "is a file extension for a shortcut file used by Microsoft Windows to point to an executable file" ("LNK File Format"). The first zero day exploit allowed the code to be spread to different computers via USB. Evidence shows that the code was first brought into the facility due to a USB drive that was infected with the malicious code. Not only did one USB drive have the code on it, but the attackers "focused their attack at five organizations in Iran that they believe would be gateways to the target" (Zetter, Kim). The second exploit took advantage of a "print spooler" vulnerability, which allowed the code to spread to other computers that are connected to the same printer. The third and fourth exploits targeted the a Windows keyboard file and a Task Scheduler file which allowed the attacker to escalate its privileges and ultimately receive administrator rights, or full control, of the machines. (Note: It was later found out that the LNX exploit had be previously used in a Trojan attack the previous year, but the zero-day was never patched. Also, two of the other exploits were posted online on blogs, but Windows never saw them to make the necessary patches for the exploits (Zetter, Kim).)

Another aspect that helped facilitate the attack was the fact that the code contained two valid digital certificates, one from RealTek and one from JMicron Technology, in its files so it was able to trick the systems in Natanz into trusting the malware as a legitimate program. It is unknown as to how the certificates were stolen, but they were another key piece of the attack to help the malware continue to be undetected (Zetter, Kim).

Once the malware was in the computer systems, it had a systematic way of finding the target, only harming the systems that matched the dossier in the code. Because of the "precise inside knowledge of the target it was seeking" Ralph Langner, a German computer security expert for Symantec, claims it is clear "that Stuxnet was the product of a well-resourced government" (Zetter, Kim). What the malware was looking for was an infected computer that had Step7 installed on it, a software program developed by Siemens. When the software was discovered, the malware would decrypt and load a Dynamic Link file, or DLL file, which contained the malicious payload of the code. Step7 was an important piece of software because it could control the Programmable Logic Controllers (PLCs), which were small computers that controlled the converters which operated the centrifuges. Normally, the commands would be given from the Step7 software to the PLC, but when infected by Stuxnet the malicious DLL file would replace the Step7 commands with its own set of commands. Furthermore, Stuxnet also "disabled and automated alarms that might go off in the system as a result of the malicious commands. It also masked what was happening on the PLC by intercepting status reports sent from the PLC to the Step7 machine, and stripping out any sign of the malicious commands" (Zetter, Kim). The centrifuges operated at 1,064Hz and received the power from the converters, but the Stuxnet code would increase the frequency to 1,410Hz and decrease the frequency to 2Hz which would damage the centrifuges. Since Stuxnet controlled the PLCs, the converters could be set to extreme high and low frequencies, yet the workers in the nuclear plant never knew that the systems were malfunctioning. "The fact that Stuxnet was injecting commands into the PLC and masking that it was doing so was evidence that it was designed… for physical sabotage" and it was evidence that Stuxnet was intended to be a targeted attack (Zetter, Kim).

Chapter 6

Cyber-crime Groups

Cyber- crime groups are one of the types of actors who are threats in the cyber world. Although there are many cyber-crime organizations that have very different strategies and structures, the primary motive of these groups is to make a profit.

Honker Union of China (H.U.C.)

Honker Union of China is a Chinese cyber-crime group that was created in late 1999 and founded by a member codenamed LION. The group has over 80,000 members and is ranked as the fifth hacker organization of the world. Of their seven known cyber-attacks, two of them have targeted the United States. The first incident occurred in May 1999 when the group hacked several US government sites. The reason for the attack is believed to be in retaliation for an incident where the United States bombed the Chinese embassy in Belgrade, Yugoslavia during the war of Kosovo in an attempt to bomb a Yugoslav military target. Although the bombing was an accident and the coordinates were incorrect, Honker Union retaliated against the United States for the incident. The other case where Honker Union attacked the United States was in April 2001 when a U.S military reconnaissance plane collided with a People's Liberation Army (PLA) naval fighter. In response to the death of the Chinese pilot, Honker Union launched a series of distribute denial of service attacks against the United States ("Honker Union of China").

Hidden Lynx

Another cyber-crime group is Hidden Lynx, which has limited information on the Internet. Hidden Lynx is a Chinese hacker for hire group that started in 2009. With and estimated of only fifty to one hundred workers in the organization, Hidden Lynx has targeted hundreds of organizations and found 3 zero-day exploits since 2011 ("Hidden Lynx – Professional Hackers for Hire"). Hidden Lynx uses extensive methods of attack and has been known for using a "waterhole" technique to carry out its attacks. The waterhole technique involves identifying sites that the target will probably visit. Once those sites are identified, Hidden Lynx will compromise those sites with code that is designed to "redirect visitors to another server that attempts to infect the victim's computer" (Lemos, Robert). The waterhole technique is an indirect way of breaching into the victim's information systems without their knowledge. In a report released by RSA, Hidden Lynx had over 32,000 systems being fed information from compromised web servers, and about twelve percent of them were infected by malware. Once the targets are infected by the compromised server, Hidden Lynx will launch an APT attack against that target (Lemos, Robert). The main purpose of Hidden Lynx's activity has been to commit cyber-espionage in specific sectors. The top six sectors that have been attacked by Hidden Lynx are information and communication systems, aerospace/defense, financial systems, energy, marketing, and government. The United States has been the target for over half of the attacks carried out by this hacker group.

Chapter 7

Hacktivist Groups

Unlike cyber-crime groups, who are motivated in their attacks by financial gain, hacktivists usually have some kind of political or social motive behind their attacks. Additionally, hacktivists try to appear to look like they are doing the right thing and try to win the favor of public opinion. Two notorious hacktivist groups are known as Anonymous and the Syrian Electronic Army (SEA).

Anonymous

Anonymous has appeared in the news for hacking many different organizations, but one thing that is unclear is whether Anonymous is a single group of hackers with a common goal, or if it is a loosely connected group of subgroups or individuals who are working under the same name. Anonymous is known for their purpose of acting as vigilante-type group on the internet, and a popular method of attack is their use of DDoS attacks. One example of their attacks was in 2010 when Anonymous launched “DDoS attacks against PayPal in response to its blockage of funds meant for WikiLeaks” (“'Anonymous' Hacker Convicted”). The reason for the attack was because PayPal refused to use their service to transfer money to WikiLeaks. Since WikiLeaks is whistle blowing website that shares secret information, which is a mission of Anonymous to prevent information filtering, the hacktivists decided to attack PayPal. Due to the attacks, PayPal claimed to have had about $5.6 million of damage (“'Anonymous' Hacker Convicted”).

Even though the members of Anonymous consider themself to be helping humanity, they have received criticism for many of their attacks. In one case though, anonymous did get a

positive response when they were able to find digital evidence to help police complete a case. A few girls were victimized by having embarrassing photos taken of them and posted on the internet, but the police could not find evidence on the suspect's computer to prove he was responsible. On the other hand, Anonymous was able to "access deleted communications" to help police bring justice to the offender (Stone, Jeff). Their power lies in the fact that they can violate the law to bring offenders to justice. This wins them popular support in some situations.

Syrian Electronic Army (SEA)

Another notable hacker group is the Syrian Electronic Army (SEA). The SEA was founded in 2011 and is a politically driven group that supports President Bashar al-Assad claiming to be a "peaceful resistance because we want only to carry the weapon of knowledge" ("About SEA"). The goal of the SEA is to spread awareness of the "truth on media and international politics pages" ("About SEA"). In doing so, SEA stays active on many social media sites and attempts to monitor information that is posted about them. SEA will hack websites and organizations that post disinformation about themselves. SEA has been known to many sites ranging from The New York Times, The Onion, Twitter, The Associated Press, Facebook pages, and more. SEA uses spamming, defacement, malware, phishing, and DoS attacks to hack its targets that are producing false information ("About SEA"). The group is believed to support President Bashar al-Assad which is why SEA has been seeing targeting western news organizations, political opposition groups, and human rights groups. One reason the SEA hacks into so many news organizations is because any time there is an article that is released about Syria that they view is inaccurate, the SEA hacks that organization they believe the information

is inaccurate or portrays Syria in a poor light. In one case, the SEA hacked Vice.com in revenge of an article that supposedly name members within the SEA.

Chapter 8

State Sponsored Cyber-warfare

While attacks may occur solely within a given country, many attacks occur between countries as well. The problem with cyber-attacks and cyber-warfare is that they the origin of the attack cannot always be proven due to limitations with network forensics. For example, attacks can be rerouted through different ports, IP addresses can be spoofed, and the use of bots can make it difficult to distinguish where an attack originated. If a nation does back a cyber-attack, but then denies any involvement, it can be very difficult to prove complicity. The problem magnifies when domestic companies and corporations are at stake of attack by another nation. When issues between two states increase, the big question is when is it time for the government of a nation to step in and take action. Similarly, if one nation attacks another nation via a cyber-attack, at which point does the attack increase in seriousness from vandalism to an act of war? What is the appropriate response? How much evidence of complicity is required before a response is warranted? The 'rules of engagement' for cyber-conflict have not yet been developed.

A recent state sponsored attack was the 'Sony hack' that occurred in 2014. The conflict began on November 24, 2014 when an organization, the Guardians of Peace (GOP) hacked to Sony Pictures Entertainment's computer system and flashed an image of a "stylized skull with long skeletal fingers" with a message on every employee's computer. The message warned that Sony had been hacked and if it did not follow the demands specified, that Sony will have its "top secrets" released (Robb, David). The hack paralyzed Sony's phone and email service, as well as its computers in New York and around the world, halting it normal business routine. Because of the attack, Sony had about 100 terabytes of data stolen, including payroll information, medical

records, workplace complaints, and email information. Guardians of Peace shared five Sony films online, four of which had not been released yet, in order to prove that the attack was real and how serious the issue was becoming. GOP continued to show the capacity of their hack when they released salaries of over 6,000 of Sony's current and former employees as well as movie budgets, confidential contracts, user name and passwords of top executives, and a list of complaints filed by employees in early December. On December 5th the hackers email Sony a threat saying:

> "Many things beyond imagination will happen at many places of the world. Our agents find themselves act in necessary places. Please sign your name to object the false of the company at the e-mail address below if you don't want to suffer damage. If you don't, not only you but your family will be in danger."

In the meantime the Guardians of Peace continued to release large dumps of private Sony information that was stolen during the hack. Kevin Mandia, Mandiant chief, reports to Sony's CEO Michael Lynton that "The bottom line is that this was an unparalleled and well planned crime, carried out by an organized group" (Robb, David). Even though North Korea praised the attack as a "righteous deed", they deny their involvement in the hack. It was not until December 16th that the hackers email Sony saying that they will attack the movie theaters that decide to show "*The Interview*," which was the first time the movie was mentioned. In response, the Department of Homeland Security (DHS) released a statement that it had "no credible intelligence to indicate an active plot against movie theaters within the United States" (Robb, David). Despite the DHS's statement, Seth Rogan and James Franco decide to cancel their promotional tour and Sony informed theater owners that they can choose not to premiere *The Interview* if they concerned about the threats. Within time several theaters including Carmike,

Landmark Theatres and others decide against premiering the movie, and Sony makes a statement that "In light of the decision by the majority of our exhibitors not to show the film *The Interview*, we have decided not to move forward with the planned December 25 theatrical release" (Robb, David).

On December 19th the FBI reported its findings "publicly that the government of North Korea was behind the Sony hack and the ensuing threats to moviegoers" (Robb, David). In an effort to appear innocent, North Korea invited the US to launch a joint investigation of the attack while stating that there will be ""serious consequences" if the U.S. retaliates" (Robb, David). After President Obama claimed the U.S. will "respond proportionally" North Korea claimed the next day that it will attack "the White House, the Pentagon and the whole U.S. mainland" (Robb, David). Because North Korea felt insulted for being accused for the attack, the representatives decided to cancel their United Nations Security Council meeting with the U.S. Also, in response to recent events, Sony decided to release *The Interview* on Christmas Day. Although not all of the movie theaters released the movie, YouTube Movies, Google Play, Microsoft's Xbox Video offered methods to rent or buy the movie.

The Sony attack is just one example of a state-sponsored attack, and how the attack was performed to achieve a political objective. When a Rand expert was asked to watch *The Interview* and give his analysis of the movie, he claimed that the movie "would have damaged Kim Jung-un internally" (Robb, David).

Chapter 9

U.S. - China Relations

As explained before, cyber-crime is "a vast array of illegal activities that are implemented via IT systems, including mobile devices" ("Who's Spying On You?"). On the other hand, cyber-warfare is when two nation states carry out cyber-attacks against one another. Cyber-warfare usually seeks to "damage state-owned infrastructure or cause damage by stealing sensitive data – rather than trying to steal money" ("Who's Spying On You?"). Cyber-warfare has become more prevalent today, such as between China and the United States; the question becomes how this should affect the relationship between the two superpowers. An attack on important infrastructure, such as the power grid or communication systems, would certainly be seen in the same context as a bombing, but what about an espionage attack against a company? Economic damage can be very real, but at what point does the government have a responsibility to step in? Even worse, what if the company had been negligent in its security procedures and was somewhat responsible for the breach?

It is important to note that I am focusing on the U.S. and China as an example, but they are not the only nations engaging in, or preparing for, cyber-warfare. Also, there is limited information available on US policy regarding cyber-warfare incident handling, specifically how or when to retaliate if at all. It is a difficult matter to determine when cyber-warfare should lead to kinetic warfare. As mentioned previously, plausible deniability plays a huge role in cyber-attacks because network forensics is not a direct science since it is easily for attackers to manipulate the metadata and reroute the attacks to appear to be coming from another location. Furthermore, it difficult for examiners to determine the source behind an attack because a state could initiate an attack, a cyber-crime or hacktivist group could initiate an attack on behalf of a

state, or a cyber-crime or hacktivist group could initiate an attack on their own behalf. The various possibilities make it difficult when determining the difference between state sponsored attacks and non-state sponsored attacks cyber-crime and cyber-warfare.

The People's Republic of China is a unique state because since it is a communist country, much of the power still lies within the government. For instance, most of the telecom networks are regulated and monitored by the Chinese government, so the information that is produced is filtered by the government as necessary.

History of U.S. – China Relations

The modern relationship between China and the United States begins in 1972 when President Richard Nixon visited China for eight days to meet with Chairman Mao Zedong. Nixon was the first U.S. president to visit China, and on his trip some of the topics he discussed included reducing the U.S. military presence in Taiwan in an effort to have China reduce its military support for North Vietnam in the ongoing Vietnam War. Although this was a great step, the early relations were a struggle because China continued to aid North Vietnam, which allowed North Vietnam to launch its Easter Offensive attack in March 1972 ("U.S. Relations with China").

In 1979 President Jimmy Carter severed ties with Taiwan, by agreeing to China's "One-China" policy, which granted full diplomatic recognition. Three months later Congress signed the Taiwan Relations Act, which allowed the U.S to resume commercial and cultural connection with Taiwan without breaching the "One-China" policy ("U.S. Relations with China"). Even though agreeing to China's "One-China" policy and the Taiwan Relations Act positively

benefitted US-China relations, incidents such as the Tiananmen Square Massacre were a problem. In 1989 after the Chinese military killed hundreds of protestors who wanted democratic changes in China, the U.S. halted its munition sales to Beijing and relations came to a standstill.

Another issue that brought about some tension with China was their human rights policy. In 1979 Wei Jingsheng, a human rights activist, was arrested and convicted because his activities were "counterrevolutionary" in China. In an effort to help improve China's human rights policy, Bill Clinton launches his policy of "constructive engagement." Within a few months of launching the policy, China decided to release Wei Jinsheng, but unfortunately he was arrested again in 2000 shortly after Beijing lost its bid to host the 2000 Olympics. After being imprisoned for four more years in various prisons, President Clinton requested the release of Wei to the United States, as well as another protestor, named Wang Dan, which helped prove some success to President Clinton's policy.

A new barrier was broken in 1996 when Taiwan held its first free presidential election and won by Lee Teng-hui of the Nationalist party. In 1995 when President Clinton invites Lee to the United States for a visit, breaking a U.S. policy that had been active for fifteen years, China stops sending ambassadors to meet with U.S. officials. About a year later, China agrees to resume exchanging officials with the U.S.

As previously mentioned, the bombing in Belgrade which the U.S. intelligence community accidentally bombed a Chinese embassy during Kosovo, thousands of Chinese citizens broke out in protests in China and damaged U.S. property ("U.S. Relations with China"). Another issue that had a negative impact on relations was the Hainan Island incident, in which a U.S. reconnaissance plane collided with a Chinese fighter pilot just off the coast of Hainan. The American crew was imprisoned for eleven days before China agreed to release them back to the

U.S. When the Chinese government demanded that the U.S. pay $1 million dollars in compensation, the U.S. decline and negotiation talks ended.

A promising development in U.S.-China relations was the U.S.-China Relations Act of 2000 which granted China "permanent normal trade relations" with the U.S. ("U.S. Relations with China"). Additionally, not long after the act was signed, China joined the World Trade Organization in 2001 ("U.S. Relations with China"). As the relations grew and became stronger over the years, so did the trade between the two countries. In 1980 US-China trade was at about $5 billion, but by the end of 2004 the trading had increased exponentially to $231 billion ("U.S. Relations with China").

Another significant even that locked the two countries together economically was when China purchased $600 billion of U.S. debt in 2008, becoming the country with the greatest holder of American debt ("U.S. Relations with China"). With the two countries so dependent on each other for trade and economic growth, it is evident that the economy of one country has a great direct impact on the other.

China's relationship with the American multinational corporation, Google, has wavered as well because of China's Internet censorship policy.

U.S. – China Cyber History

One of the most controversial hacker groups is APT1, also known as Comment Crew, Comment Group, Unit 61398, and possibly Shady Rat. APT1 is a hacker group that is based primarily in China and according to a report that was completed by the Mandiant group, one of their reports, the Mandiant Report virtually proves that China is sponsoring APT1 is one of over

20 APT groups in China and Mandiant believes APT1 receives direct government support the Chinese government. APT1 is a sophisticated and well funded hacker group that has been and still is launching APT attacks and stealing information from over 140 organizations. APT1 most commonly uses spear phishing attacks (a social engineering attack) for the initial compromise. From there the attacker continues through the phases of an APT attack and begins stealing information. At the release of the Mandiant Report, of the 142 total victims of APT attacks, the United States made up 115 of those victims. Of all of the attacks recorded and published in the Mandiant Report, the top five sectors of attack were IT, aerospace, public administration, satellites and telecommunications, and scientific research and consulting. APT1 has stolen hundreds of terabytes of data since at least 2006 when it began its APT attacks (Sanger and Perlroth).

Although APT1 could be an organization acting on behalf of its own interest rather than for the government of China, the Mandiant report contains conclusive evidence that show that APT1 is a state sponsored cyber-organization also known as Unit 61398. Unit 61398 is "considered by China to be a state secret" and is known to be located on "Datong (大同路) road in Gaoqiaozhen (高桥镇), which is located in the Pudong New Area(浦东新区) of in Shanghai （上海） (APT1). The facility was constructed in 2007 and is twelve stories tall. The building's infrastructure has fiber optics which is provided by China Telecom and is said to be used for national defense. Of the four networks that Mandiant has traced back to APT1 in Shanghai, two of the networks give service to the Pudong New Area, which is where Unit 61938 is located.

What makes APT1 a unique organization is that it has successfully "systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously" (APT1). The group

has a well planned out methodology that revisits its compromised targets over several months or years with the intention of stealing large quantities of information. Mandiant has data showing that APT1 has had access to a victim's network for an average of about 356 days with the longest being four years and ten months. Furthermore Mandiant has seen APT1 steal "6.5 terabytes of compressed data from a single organization over a ten-month time period" (APT1).

Not only does ATP1 have a well developed methodology, but also it has an extensive computer infrastructure globally. In the last two years that Mandiant observed APT1 "establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries" (APT1). Also, of the "767 separate instances in which APT1 intruders used the "HUC Packet Transmit Tool" or HTRAN to communicate between 614 distinct routable IP addresses and their victims' systems … 614 (100%) were registered to China, [and] 613 (99.8%) were registered to one of four Shanghai net blocks" (APT1). Due to all of the evidence gathered by Mandiant over is years of observing ATP1, they have concluded that because so much of the networking traffic has been traced back to the location of where Unit 61398, APT1 is Unit 61398, although they admit the other unlikely possibility that APT1 is a

> "secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission" (APT1).

APT1 is just one example of how China has participated in cyber-crime against the United States, but the U.S. is not innocent of reciprocating such activity.

One example of the U.S. hacking into Chinese organizations was found out when Edward Snowden, a whistleblower who worked as a contractor for the National Security Agency (NSA),

leaked tens of thousands of classified documents. The Chinese telecommunication company Huawei serves on third of the world's population, and because of the Snowden leaks it became known that the NSA had exploited Huawei's technology to be able to monitor China. Not only did the NSA gather the information to learn about China's activity, but it allowed the U.S. to monitor countries who do not purchase U.S. products because the NSA already had a way into the Huawei's servers so it could monitor network traffic to those countries. Furthermore, when Huawei constructed undersea cables to connect to some of its prime customers, the U.S. saw it as a great way to monitor high priority targets as well, such as Iran, Afghanistan, Pakistan, Kenya, and Cuba (Sanger and Perlroth).

Another instance of the U.S. hacking China occurred in January 2013 when the U.S. hacked into Tsinghua University in Beijing, which hosts "one of China's six major networks that contains data on millions of Chinese citizens" ("U.S. Hacked China Universities"). This information was leaked by Snowden as well and it became clear that the U.S had been spying on China and Hong Kong for years.

Although China and the United States both do participate in cyber-warfare, the intentions of the two countries are quite different. James A. Lewise, a computer security expert at the Center for Strategic and International Studies in Washington describes that "China does more in terms of cyber-espionage than all other countries put together" (Sanger and Perlroth). On the other hand American officials have reported that the U.S. only hacks for the purpose of national security measure, not for corporate theft. White house spokeswoman Caitlin M. Hayden said: "We do not give intelligence we collect to U.S. companies to enhance their international competitiveness or increase their bottom line. Many countries cannot say the same" (Sanger and Perlroth).

Chapter 10

Internet Regulation and Policy

One of the most challenging aspects about the Internet is that there is no international governance of cyber-activity. Even within a country such as the United States, because the Internet is such as recent development, regulation has not caught up yet to fully govern the actions of cases where cyber-activity is involved. One of the main issues that the United States is trying to pursue is to clarify the "threshold of attacks that constitute an act of war" (Segal, Adam). A second issue is to promote "digital safe havens" (Segal, Adam). While the U.S. has the intention of "defining the rules of interstate behavior in cyberspace," similar to the formalized conventions of the Geneva Protocols, it difficult to get many countries to agree on at which point a "cyber-attack becomes the equivalent of an "armed attack" in international law as well" (Segal, Adam). Defining when a cyber-attack calls for necessary "kinetic effects" as well as determining whether the target of the attack is critical enough to call for measures for the government to step in still remains to be clearly developed and agreed upon.

Another issue is that China and Russia "see the free flow of information as a threat to domestic stability," which is why they are likely to demand that the United States limit its "digital activists" in order for them to give in to the demands of the U.S. such as controlling the "patriotic hackers" (Segal, Adam). The reality is that the U.S. is unlikely the meet these demands because of the power and support of the First Amendment of the U.S. Constitution. Being unable to see eye to eye on the two issues is just one example of why it is so difficult for an international standard to be reached.

The U.S government is trying to get close allies to support negotiations for international Internet regulation. By getting countries within the United Nations, G20 and other regional

groupings involved and supportive of the regulations, the U.S. will have leverage on China and Russia in the hope that they will support the regulations. Unfortunately, one of the key issues that hinder the U.S. from gathering support is that after Stuxnet, “it is now widely assumed that the United States, along with Israel, was behind the code” so “many countries will remain skeptical about Washington’s intentions” (Segal, Adam).. But if the U.S. can gain the necessary support, its allies have agreed that an appropriate first step is to “issue a public “cyber declaratory statement” that reserves the right to respond through a conventional or computer network attack, but leaves some room for maneuver.” With a public statement, other countries will know where the United States stands and how it will react to attacks and it could gain support and create a common understanding amongst nations.

Chapter 11

Future Outlook

The threat of cyber-attacks is a real issue and is something that needs to be addressed quickly. As Stuxnet, the 'Sony hack' and other incidents showed, cyber-attacks have the capacity to not only damage an organizations reputation, but also have the capacity to cause physical damage. Some of the laws the United States, as well as other countries, should look to ratify are laws that bring justice to hackers who are attacking other countries. Creating legislative punishment for such actions could reduce the number of international attacks, and be able to improve relations with other countries. Another law that the United States may want to pass is one that makes it illegal for mobile and computer devices to not have anti-malware software installed. Some people may complain that it is a method for the government to spy on people, but the reality of the matter is that it will reduce the spread of malware and limit the amount of damage that people face from being vulnerable to attacks. If the United States is unable to adapt to the developing technological world, then the outlook for its future looks very unsettling.

A realistic, yet devastating attack that the U.S. could face in the near future is an attack on its critical infrastructure. One example of such an attack would be if a cyber-weapon took out a power plant. Not only would that create a problem because people would be without power for a period of time, but the bigger issue would be how to appropriately respond to such an attack. If an attack to that caliber physically damaged valuable infrastructure such as an electric power plant, then the U.S. would have to decide if it was going to respond back with a cyber-weapon or with kinetic warfare. Our infrastructure is a valuable necessity that is at risk, and if the U.S. does not take the necessary precautions to protect ourselves and mitigate our risks, we could endure facing a critical situation that could amount to cyber or kinetic warfare.

Conclusion

The capability of cyber-attack has grown tremendously over the past 30 years. Advanced attacks such as Stuxnet show how damaging cyber-attacks can be, and with people constantly developing and reconstructing malware code, the future of cyber-attacks and cyber-warfare is devastating. International cooperation will need to happen to some degree to help suppress the current warfare, but it will require all sides to give and take to find a common ground. In our modern and digital society, civilian targets and national security are vulnerable to cyber-attacks that could inevitably instigate kinetic warfare. The security of cyberspace is at risk and needs to be properly secured and regulated to prevent a doomsday from occurring. Malware is out there and our future is at stake. Many people like Lieutenant General Keith Alexander, director of the National Security Agency, claim that "the next war will begin in cyberspace," so it is imperative that the United States takes necessary action and is prepared (Lopez, Todd C.).

BIBLIOGRAPHY

"About SEA." *Syrian Electronic Army*. Syrian Electronic Army, 2015. Web. 07 Apr. 2015.

"Advanced Persistent Threats: How They Work." *Symantec*. Symantec Corporation, 2014. Web. 24 Nov. 2014.

Anderson, Nate. "Massive DDoS Attacks Target Estonia; Russia Accused." Ars Technica. Condé Nast., 14 May 2007. Web. 31 Mar. 2015.

"'Anonymous' Hacker Convicted over WikiLeaks Revenge Attack on PayPal." RT News. RT, 6 Dec. 2012. Web. 04 Apr. 2015.

APT1. Mandiant, 18 Feb. 2013. Web. 1 Sept. 2014.

Beal, Vangie. "DoS Attack - Denial of Service Attack." Webopedia. QuinStreet Inc., n.d. Web. 11 Apr. 2015.

"Bots and Botnets—A Growing Threat." *Norton*. Symantec Corporation, 2015. Web. 24 Mar. 2015.

Cerf, Vint. "Internet Society." Brief History of the Internet. Internet Society, n.d. Web. 11 Apr. 2015.

Criddle, Linda. "What Is Social Engineering?" Examples and Prevention Tips. Webroot Inc., 2015. Web. 30 Mar. 2015.

"Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. George Washington University, n.d. Web. 24 Mar. 2015.

"Estonia vs. Russia: The DDOS War." (n.d.): n. pag. Birmingham InfraGard, June 2007. Web. 3 Nov. 2014.

G, Tim. "Renting a Zombie Farm: Botnets and the Hacker Economy." Renting a Zombie Farm: Botnets and the Hacker Economy. Symantec Corporation, 8 Aug. 2014. Web. 24 Mar. 2015.

"Hidden Lynx – Professional Hackers for Hire." *Security Response Blog*. Symantec Corporation, 7 Sept. 2013. Web. 8 Oct. 2014.

"History of the Web." *World Wide Web Foundation*. World Wide Web Foundation, 2015. Web. 15 Mar. 2015.

"Honker Union of China to Launch Network Attacks against Japan Is a Rumor." *ChinaHush*. ChinaHush, 15 Sept. 2010. Web. 4 Jan. 2015.

Ingram, Mike. ""Love-Bug" Virus Damage Estimated at $10 Billion." *World Socialist Web Site*. World Socialist Web Site, 10 May 2000. Web. 22 Feb. 2015.

"Internet Threat Report 2014." Trends 19 (2014): 9-77. Web. 30 Dec. 2014.

"Internet Timeline." Fact Monster. Pearson Education, Inc, 2014. Web. 23 Mar. 2015.

Kabay, M. E. "A Brief History of Computer Crime: An Introduction for Students." (2008): 5-11. Web. 9 Jan. 2015.

Kirk, Jeremy. "Click Fraud Botnet Defrauds Advertisers up to $6 Million." Computerworld. Computerworld, Inc., 20 Mar. 2013. Web. 20 Nov. 2014.

Lemos, Robert. "Government Agencies, Utilities Among Targets of 'VOHO' Cyber-Spy Attacks." EWeek. QuinStreet Inc., 2012 Sept. 27. Web. 24 Mar. 2015.

Lopez, Todd C. "Next War Will Begin on Cyberspace, Experts Predict." Www.Army.mil. The United States Army, 27 Feb. 2009. Web. 07 Apr. 2015.

Menninger, Marc. "The First Internet Worm & Internet Worm Virus." The First Internet Worm & Internet Worm Virus. Streetdirectory, 2015. Web. 24 Mar. 2015.

Musa, Sam. "Advanced Persistent Threat - APT." Academia.edu. Academia, Mar. 2014. Web. 24 Mar. 2015.

Nahorney, Ben, and Nicolas Falliere. "Trojan.Zbot." *Symantec*. Symantec Corporation, 10 Jan. 2010. Web. 13 Jan. 2015.

Peter, Ian. "History of the World Wide Web." *Net History*. The Internet History Project, 2004. Web. 24 Mar. 2015.

Robb, David. "Sony Hack: A Timeline." Deadline. Penske Business Media, LLC, 22 Dec. 2014. Web. 11 Apr. 2015.

"Rootkit." Wikipedia. Wikimedia Foundation, 7 Apr. 2015. Web. 11 Apr. 2015.

Rouse, Margaret. "Bot (robot) Definition." SearchSOA. TechTarget, 2015. Web. 20 Jan. 2015.

Rouse, Margaret. "LNK File Format." LNK File Format. WhatIs.com, July 2010. Web. 11 Apr. 2015.

Sanger, David E., and Nicole Perlroth. "N.S.A. Breached Chinese Servers Seen as Security Threat." The New York Times. The New York Times, 22 Mar. 2014. Web. 19 Dec. 2014.

Segal, Adam. "Cyberspace Governance: The Next Step." Council on Foreign Relations. Council on Foreign Relations, n.d. Web. 31 Mar. 2015.

"SonicALERT: Gone with the Wings NgrBot Dropper (Oct 4, 2013)."*MySonicWALL*. Dell, 4 Oct. 2013. Web. 1 Mar. 2015.

Stone, Jeff. "What Is Anonymous? 'Hacktivist' Involvement In Mike Brown Shooting Proves Vigilante Justice Is Now Routine." International Business Times. IBT Media Inc., 15 Aug. 2015. Web. 04 Apr. 2015.

"Trojan Dropper." *Symantec*. Symantec Corporation, 2015. Web. 12 Dec. 2014.

"U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press." Forbes. Forbes, 22 June 2013. Web. 14 Nov. 2014.

"U.S. Relations with China." Council on Foreign Relations. Council on Foreign Relations, n.d. Web. 11 Apr. 2015.

"What is a Rootkit." What is a Rootkit. AVG Technologies, n.d. Web. 11 Apr. 2015.

"What is the Difference: Viruses, Worms, Trojans, and Bots?" Cisco. Cisco, n.d. Web. 3 Jan. 2015.

White, Kelly. "The Rise of Cybercrime 1970s - 2010." Slideshare, 2013. Web. 24 Mar. 2015.

"Who's Spying On You?" Kaspersky Lab, 2013. Web. 2 Jan. 2015.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History | WIRED." Wired.com. Conde Nast Digital, 11 July 2011. Web. 11 Apr. 2015.

ACADEMIC VITA

Jacob Sisko
1104 Amber Lane
Lansdale, PA 19446
jds5619@psu.edu

EDUCATION:

The Pennsylvania State University — University Park, PA
College of Information Sciences and Technology
Schreyer Honor's College Gateway Program
B.S in Security and Risk Analysis, Cyber Security option
Minor in Information Science and Technology
Minor in Chinese (Mandarin) — Expected May 2015

CIEE Study Abroad: Shanghai- Accelerated Chinese Language
Summer 2013
Completed two months of study in an accelerated Chinese language and culture course in Shanghai. Lived with a Chinese roommate and traveled around to different cities in China learning about the culture.

Cyber Corps; Scholarship for Service- an education and professional development program for emerging leaders, sponsored by the National Science Foundation (NSF), U.S. Office of Personnel Management (OPM), and Department of Homeland Security (DHS).

Strategic and Global Security Program, an Intelligence Community CAE- a Title 50 Intelligence Officer Training Program, sponsored by the Office of the Director of National Intelligence (ODNI).

Schreyer Honor's College Scholar- As a student of the honor's college in the gateway program, I am required to take fourteen credits of honor's classes as well as write a thesis. My thesis focuses on the history of cyber crime and cyber warfare, how cyber warfare impacts U.S. China relations, and the outlook of cyber warfare in the future based on the growing capability of cyber attacks.

IST Diplomats- an education and professional development program for the College of IST, where I am a representative of the college of Information Science and Technology (IST) at special functions and give tours of the college to prospective students, alumni and others interested in the college.

COURSEWORK PROJECTS:

IST 451 – Network Security

- Used various tools on a virtual machine to complete class labs for pen testing. Used Wireshark to retrieve network traffic, used nmap to scan the network ports and Nessus to conduct vulnerability tests on open ports.

IST 454 – Computer and Cyber Forensics: Team leader of the Final Project

- Demonstrated cracking the password of a network using a dictionary attack with the Aircrack-ng tool on BackTrack 5, and cracked the router administer setting using the Hydra tool in order to reconfiguring the router settings.

SRA 221- Overview of Information Security: Next Century Application Development Project

- Completed the coding of an application used for first responders, as the team leader of the project. Using javascript, the team created a secure authorization and authentication system.

SRA 231- Decision Theory and Analysis: Metro Crash Simulation Capstone Project

- Successfully completed the simulation to investigate the incident as the team leader of the group, acting in the role of the FBI.
- Used a decision theory matrix, Analyst's Notebook, and Analysis for Competing Hypotheses (ACH).

SKILLS:

- Pen testing tools: Wireshark, Backtrack 5, nmap, Nessus, aircrack-ng, metasploit
- Analytic tools: GIS, Analyst's Notebook, Analysis for Completing Hypotheses (ACH)
- Chinese: Intermediate speaking, listening, and writing, completed seven semesters of Chinese
- Programming: One course in each Java Language and C++
- First aid certified (Jan. 2014- Jan 2016)
- CPR/AED certified (Jan 2014 – Jan 2016)

WRITING & PRESENTATIONS/BRIEFINGS:

- Participated in a simulation at the Army War College where I acted in a group as the role of the PA state government and responded to a foreign nation cyber attack on the US. As a team we developed a course of action, and explained the effects and outcomes. At the end I gave a briefing representing our group in front of the students, professors, and government agency officials.
- Participated in two simulations at Penn State led by the CIA, "Pearl Harbor" and "Iranian Elections." After my group was given intelligence reports, we had to analyze the reports, and write a BLUF (bottom line up front) report. Then I gave a "brief the president" presentation on our knowledge and answered his questions supporting my answers with the intelligence reports.

WORK EXPERIENCE:

Intern for **Ernst & Young in Information Technology Risk and Assurance** Summer 2014

- Performed two months of staff level work as a full-time intern at both Automated Data Processing (ADP) and CACI International Inc. client sites.

- Mapped data flows, wrote professional documents, participated in interviews, performed security auditing such as reviewing and testing user access privileges, password security and user policies.

Pennsylvania Criminal Intelligence Center (PaCIC) Spring 2013

- Conducted research about ten hours a week during the semester on street gangs in Pennsylvania; defined what a gang is, created a threat matrix, and created threat analysis chart of the most dangerous gangs in PA.
- Gave a presentation on our progress and results from the semester.

Strategic Intelligence Research Internship Fall 2013

- Participated in a research project on the economics of crowd-sourced/state developed cyber weaponry with a specific approach of botnets and black market malware
- Delivered the presentation to General James Cartwright, USMC, Retired, former Vice Chairman of the Joints Chiefs of Staff

Intern for the International Center for the study of Terrorism (ICST) Summer 2012

- Conducted research for Dr. John Horgan, in a research product funded by the Department of Homeland Security, Study of Terrorism and Responses to Terrorism, and the Office of Naval Research
- Assisted and promoted the scientific study of terrorism and political violence in the radicalization and recruitment project which examined the factors that lead individuals to become involved in, and disengage from terrorist networks.
- Wrote a case study report on former terrorist Thomas Tarrants III of the Ku Klux Klan

Life Guard at Towamencin Community Pool Summers 2008-2011

- Worked thirty hour weeks as a life guard. Responsible for opening and closing shift duties, as well as helping with the pool maintenance. Received life guard, first aid, CPR, and AED training

Swim instructor 2008-2009

- Trained children ages 5-10 in pre-beginner and beginner swim lessons. In a group of 5-8 children, I would teach them the basics skills of swimming ranging from various floats, kicking and some freestyle skills.

ACTIVITIES:

- **Men's Water Polo president, vice-president, and captain**- I was the men's vice president 2012-2013, president 2013-2014, and captain 2012-2014. As vice-president I helped the president carry out his duties. Also, I wrote bulletins and letters to be sent out to the alumni to help raise money and to keep the alumni informed about our season. As president, I was the liaison between our team and the club sports administrators. I had to manage and organize all paperwork (participation agreements, liability waivers, insurance, etc.) schedule our practices and tournaments, and communicate with the current and new members about upcoming events and practices for the season. As captain I worked with the other captains to coordinate the practice, and lead the team through it, while helping the players. During games and tournaments we would decide who would play and lead the team in and out of the pool.
- **Lion Ambassadors**- I take alumni and incoming freshman around campus at Penn State and give them a tour of the university. Also, I help put on events for our university for the students to attend.

- **Women's Water Polo coach**- I have been the women's water polo coach from 2013-2015. As the coach I would act as the speaker for the captains of the women's team to run the practices. I would give feedback to help players improve, and coach the team by giving them a strategy for their games.
- **Security and Risk Analysis (SRA) Club Corporate Relations Chair**- During the 2012-2013 school year I was the Corporate Relations Chair where I represented the club at IST sponsored events, and I helped reach out to bring in speakers for our club meetings.
- **Information Assurance club**- I was a club member of a group that gave presentations on pen testing techniques, ranging from vulnerability scans and other white hat hacking techniques. We had guest speakers come in and give demonstrations on topics relevant to their field as well.
- **Penn State Athletes Take Action**- Volunteer program where students go into elementary schools to talk about anti-bullying with 6th grade students. I lead a one hour presentation to make the students more aware about bullying, interact with them, do activities, and teach them about how to prevent bullying.

AWARDS/RECOGNITION:

- **Most Valuable Player:** Collegiate Water Polo Association (CWPA) ranked me as the MVP of the Mid-Atlantic Division in 2014 season.
- **First Team:** CWPA ranked me as one of the top seven players of the Mid-Atlantic Division in 2014 season.
- **8th Place at Nationals:** I was one of the starting players of the team that finished 8th at Nationals in Salt Lake City, Utah in the 2014 season.
- **Second Team:** CWPA ranked me as one of the top seven players of the Mid-Atlantic Division in 2013 season.
- **11th Place at Nationals:** I was one of the starting players of the team that finished 11th place at Nationals in Portland, Oregon in the 2012 season.