2015-04-10

Cybersecurity and the Future International Competitiveness of the United States

Tai Gray
Brigham Young University - Provo, taigray@gmail.com

Follow this and additional works at: https://scholarsarchive.byu.edu/studentpub

Part of the Political Science Commons

BYU ScholarsArchive Citation
https://scholarsarchive.byu.edu/studentpub/220

This Class Project or Paper is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in All Student Publications by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.
CYBERSECURITY AND THE FUTURE INTERNATIONAL COMPETITIVENESS OF THE UNITED STATES

Tai Gray
International Relations Capstone
April 10, 2015
Introduction

The United States of America has long been considered fertile ground for experimentation, innovation and invention. America is the home of the airplane, the assembly line model for the production of goods, and other successes that have revolutionized the world and built up the American economy. The United States was also one of the first to make significant advances in the cyber realm. During the 1990’s and 2000’s, an increasingly large number of Americans started using advanced computer hardware, software, and networking capabilities to achieve what previous generations thought to be impossible. Since 2000, well over two million patents have been filed in the United States alone, demonstrating rising levels of innovation and technical achievement.¹ Such advances have been key to the growth of the U.S. economy and continue to influence America’s standing in the world order.

While breakneck technological advancements have no doubt contributed to the rise and continued prosperity of the United States, they also give rise to new challenges and dangers. Unlike the physical world, where geography and the laws of nature prevent mobility, events in the digital realm occur almost instantaneously. While speed can be an advantage for things such as online communication and data transfers, it comes with the cost of decreased defense and protection. While the world has had millennia to perfect means of physical protection, the digital world has had only a few decades. This disparity becomes an important issue when considering the current pervasive state of interconnected technologies; the global network of interconnected devices is estimated to include over two billion people with approximately 12 billion connected devices, ranging from industrial servers to web-enabled...

As humanity has come to rely more on digital devices for the operation of daily life, disruptions in the network can be extremely inconvenient, even damaging. We live in a world where massive amounts of data of all kinds are created and stored every minute of every day, whether it be a family’s vacation photos or a multinational bank’s transaction records; when such virtual data is misplaced, misused, or destroyed, very real consequences ensue. The loss of banking information can cost millions to repair, the abuse of personally identifying information can force individuals into bankruptcy, and the leak of sensitive military data can endanger the lives of citizens and those protecting a country’s national interests.

As the world’s only superpower, the United States has a plethora of domestic and international interests that are vital to the maintenance of society and the continued development of the country. The security of these interests hinges on the ability to both prevent and recover from various sorts of computer attacks. During the past decade, the U.S. government has increasingly focused on the protection of such assets by conducting policy and standards reviews, hardware and software inspections, as well as research and development of defensive and offensive cyber tactics. However, a chain is only as strong as its weakest link. Many government and military networks are intertwined with public networks, introducing vulnerabilities to previously secured systems and placing key resources at risk of attack. Additional action must be taken to strengthen national networks at the grassroots level, ensuring the adoption of best practices by both private businesses and individuals while providing the tools and resources necessary to harden targets against future attacks. To achieve these ambitious goals, the public and private sector must work hand in hand while

maintaining the delicate balance between civil liberties and increased security. Many steps have already been taken in the right direction, but future policies must be altered to include more participation from the end users of technology. This paper will examine the state of cybersecurity based on current events and ongoing discussion among policy makers and scholars in the field of cybersecurity. My research indicates that cybersecurity is inseparably connected to the future international competitiveness of the United States and must play a more significant role in both governmental and private spheres of American society. To increase the strength of U.S. cybersecurity and defend against future attacks, the government should devote more resources to providing cybersecurity tools and information to the public, promoting the implementation of secure forms of communication and purchasing, as well as researching and developing both offensive and defensive cyber tools. By focusing efforts on these three key areas, the U.S. government can better prepare for future cyberattacks and minimize risk to both public and private entities.

Globalization and the Proliferation of Technology

Globalization is the mixing force of the world, the product of constant international and intercultural exchange that turns the world into a giant melting pot. Globalization is fueled by two objectives, the need for new experiences and the desire for gain. Mankind is very creative, and thus is in an almost constant search for sources of inspiration to satisfy natural curiosity and the need to leave the familiar. This tendency contributes to globalization by encouraging travel to new destinations and seeking new experiences, which are then spread to others either directly or indirectly. However, the second objective, that of monetary gain, has traditionally been the primary goal of globalization. Endeavors such as the Silk Road and the exploration of the West have largely been products of business ventures designed to bring more capital to the mother country while exchanging goods along the way. This tendency
toward international trade as a source of income has only become stronger over the past few centuries and international trade has become vital to the survival of many countries.

An important aspect of recent globalization has been the spread of technology, particularly advancements in digital communication and data usage. The advent of the computer revolutionized the way work around the world was done, and the creation of a network to connect digital devices brought the world together in an unprecedented way. Instead of requiring months of waiting to communicate across oceans or continents, communication through email is nearly instantaneous. New technological advances combined with the recent economic growth enjoyed by the majority of countries around the world enabling them to gain access to these technologies has contributed greatly to the bridging of gaps between civilizations. The world has become intertwined.

The Role of Computer Security in Everyday Life

With a more interconnected network of users, there will always be people who hope to use these new developments for corrupt purposes. As a society, we have grown dependent on technology for the functioning of everyday life: many rely on smartphones to wake them up in the morning, online banking to manage their finances, email for communication, and databases to store customer information. Governments not only rely on computer systems to manage public works like water and electricity, satellite imagery and global positioning for advancing military goals, and secure lines of communication to maintain relations with other countries. Without the proper precautions, no information would be private and no technology could be guaranteed to work properly. Security helps to establish trust, which in turn increases our productivity and effectiveness as we use timesaving technologies. However, when security fails, the results can range from inconvenient to devastating. All technologies are inherently at risk of attack and misuse by cyber criminals and hostile governments, which
increases the demand for security and safety. In order to understand the importance of cyber security, we must first understand the potential risks that come from various types of malicious cyber behavior. By better understanding the risks involved with technology, all can better assure that risks can be averted and attacks prevented.

_Potential Threats to Computer Security_

There are many different kinds of cyber criminals who can influence the security of a network or system. First, there are the basic black hat hackers, those whose intent it is to cause harm to a system or gain access to private information. There is a lot of variety within this designation. Some hackers create viruses to tamper with computer systems for the sake of proving that it can be done. Some use methods such as spear-phishing and social engineering (using spam emails or social interaction to gain access to private information) to obtain information like social security numbers or credit card information in order to steal money from the victim. Others develop advanced viruses that can infect and destroy a user’s files.

Second, there are hacktivists, patriotic hackers that use their abilities to further the objectives of a group or organization through various means. Hacktivists may have more support, either from a group or from a larger organization, and thus can have a more significant impact on their targets. Third, there are state actors, a group of hackers that is sponsored by a nation-state for the purpose of advancing that state’s agenda through the use of cyberattacks. This type of hacker is the most dangerous, as he or she often has significant monetary and technical resources with which to conduct his or her attacks. The purposes of attacks can also be varied, whether it be crippling another country’s computer networks, stealing state secrets and intellectual property, conducting espionage on the leaders of a country, etc.

---

The United States faces significant threats from all of these sources; however, state actors and large groups of advanced hackers are the primary concern of the government and business leaders. There are several countries currently involved in a sort of cyber war with the United States: in order of increasing capability, they are North Korea, Iran, China, and Russia.

Figure 1. Cyber threats to the U.S. homeland, in U.S. House, Cyber Threats from China, Russia, and Iran, 16.

Figure 1 depicts the current intentions of each of the four nations towards the United States in regards to cyber policy, compared to their capability to successfully conduct attacks on American computer infrastructure. The circles represent “traditional, economic, and industrial espionage” while the diamonds represent “activities that alter (disrupt, destroy, etc.) the targeted data/information”. Beginning with North Korea, the diagram shows that it has relatively little capability to successfully conduct cyberattacks on the United States, but that it intends to use attacks to destroy rather than for espionage. This is consistent with the recent cyberattacks on Sony Pictures in December of 2014, which President Obama has declared was

---

4 U.S. House. Cyber Threats from China, Russia, and Iran, 16.
the work of the North Korean government sponsored hackers.\(^5\) Iran puts more effort into destructive attacks and has much more advanced capabilities than North Korea. It has a so-called “Cyber Army,” sponsored by the Iranian government, who regularly conducts attacks on the U.S. financial industry and other important targets.\(^6\) Several officials have speculated that the increase in Iran’s attacks is in retaliation to U.S. opposition to its development of a nuclear program.\(^7\) Recently, a group suspected to be sponsored by Iran attacked Aramco, a Saudi Arabian oil company, destroying approximately 30,000 computer hard drives and rendering the entire system useless.\(^8\)

On the other end of the spectrum displayed in this graph are Russia and China. These two countries have very significant cyber capabilities, approximately equal to those of the United States, but they are more interested in using attacks for espionage than to cause physical damage, though physical damage is not out their reach. Russian cyberattacks do not appear in the news very often, but Russia has demonstrated its ability to use them effectively while incapacitating the states of Estonia and Georgia\(^9\), especially during the time preceding the land invasion of Georgia.\(^10\) China, on the other hand, has primarily been using cyberattacks in order to conduct espionage, compromise government and business networks, and steal


\(^6\) U.S. House, *Cyber Threats from China, Russia, and Iran*, 26.


\(^8\) U.S. House, *Cyber Threats from China, Russia, and Iran*, 35.

\(^9\) Ibid., 7.

intellectual property from U.S. companies.\textsuperscript{11} Due to each country’s significant budgets set aside for the sole purpose of enhancing competition though conducting cyberattacks, these four nations pose a significant threat to the future competitiveness of the United States.

While not within the scope of this paper, it is also important to address the possibility of cyberterrorism. The capability to commit acts of cyberterrorism exists, but is currently relegated to the countries with advanced cyber resources available at their disposal. While cyberattacks are certainly common, and many of them cause destruction to personal property, the word cyberterrorism entails a new dimension of attack, one that results in violence being used against people in order to create fear for a larger, often politically-motivated purpose through the use of technological means.\textsuperscript{12} The vast majority of cyberattacks are either unsuccessful or do not result in the significant disruption or damage of vital infrastructure systems and thus do not qualify as cyberterrorist attacks. As of yet, there have not been any examples of cyberterrorism, though some attacks demonstrate the possibility of such attacks in the future.\textsuperscript{13} The STUXNET worm, created in 2010 by the National Security Agency and Israel in an attempt to destroy Iran’s ability to develop a nuclear program, is perhaps the closest example of cyberterrorism.\textsuperscript{14} The worm was specifically designed to allow remote access to


\textsuperscript{12} “To qualify as terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.” Gabriel Weimann, “Cyberterrorism: How Real is the Threat?” \textit{United States Institute of Peace}, December 2004, http://www.usip.org/sites/default/files/sr119.pdf (Accessed April 11, 2015): 4.

\textsuperscript{13} Ibid., 1.

industrial control systems, in this case the centrifuges inside of Iran’s nuclear reactors.\textsuperscript{15} With remote access, the controller could then send instructions to the centrifuges and make them spin at dangerously high speeds, resulting in the overload of the system and the destruction of the machinery. This attack was mostly successful, with many machines incapacitated and Iran’s nuclear program put on hold. However, had this attack caused explosions which could have killed civilians, it could be counted as a terrorist attack. Other attacks aimed at causing the physical malfunction of necessary machinery, such as a system controlling the flow of water from a dam, could qualify as cyberterrorist attacks if the attack is successful and innocent people were harmed for a political purpose, but no such attack has yet taken place.

\textit{Economic Effects of Cyberattacks}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{incidents.png}
\end{figure}

As technology becomes more prevalent and the world better understands how to use it to its full potential, the number of cyberattacks has risen. As seen in figure 2, the number of cyberattacks reported to government agencies that specifically handle attacks has risen dramatically just over the past decade, illustrating an overall growth in the number of attacks in general. From 2006 to 2012, there was an average increase of 150 percent each year in the number of attacks reported to this one agency, with the growth rate leveling off at the year 2010. Since 2002, there has been an 82 percent increase in the number of computer intrusion investigations at the Federal Bureau of Investigation (FBI). This is due to two factors: the rapid advances made in technology (and, thus, offensive capabilities) and the difficulty of protecting every target from an attack. Each of these attacks demonstrates a significant financial loss to both the individual company being attacked as well as to the overall U.S. economy. According to the most recent report from Symantec, a private company specializing in computer security, the “total number of breaches in 2013 was 62 percent greater than in 2012.” The breaches referred to here are attacks specifically made on businesses with the intention of stealing data and personal information of customers, which can later be used to open new credit cards, file insurance claims, transfer money, or even be compiled into lists to be sold on the black market for others to exploit. These breaches are extremely significant, both to the companies being breached and to the individual customers having their personal information stolen. According to Symantec, “eight of the breaches in 2013 exposed more than 10 million identities each,” including “credit card information, government ID numbers, home addresses, medical records, email addresses, login, passwords” and other information. These

---

16 U.S. House, Protecting Your Personal Data, 18.
18 Ibid.
breaches negatively affect many aspects of a business’s daily operation. They suffer the reputation costs of not having been able to defend important information from a cyberattack (especially if the breach is heavily publicized by the media), they could be sued, and they have to pay for the detection of the breach, the escalation, and for whatever means they use to compensate their customers.

A potent example of the costs associated with a large data breach is the breach experienced by Target that was discovered in December of 2013.\textsuperscript{19} The information for over 110 million customers was stolen by hackers who installed malware on Target’s point-of-sale network. The story was brought to light and taken up by the media, resulting in a major outcry from the affected consumers.\textsuperscript{20} Target suffered a significant decrease in sales during the busy Christmas season, in addition to the costs of computer forensics needed to research and eliminate the threat in its systems. Recently, Target made a settlement with the affected customers for $10 million to cover damages. In the end, a report from the Consumer Bankers Association and Credit Union National Association estimated Target’s total losses to be over $200 million, not including the $100 million that Target said it would spend to update its systems with more security features.\textsuperscript{21}

The Target case was obviously one of the largest breaches of the year 2013, and the costs were very significant. However, costs also exist for smaller businesses.


\textsuperscript{21} Meagan Clark, "Timeline of Target’s Data Breach and Aftermath."

Figure 3 shows the proportion of spear-phishing attacks directed at each business size (as mentioned before, spear-phishing is a method by which hackers gain personal information or information from which they can conduct further cyberattacks). While large companies definitely receive the brunt of total spear-phishing attacks (due to their great resources and valuable assets), small businesses are the targets of a significant number of attacks as well. This could be due to the businesses’ lack of protections against cyberattacks, making the probability of a successful attack increase. According to a report from the National Cyber Security Alliance and Symantec, “20 percent of cyberattacks are on small firms with less than 250 employees” and “40 percent are focused on firms with less than 500 employees.”22 This

report found that there was a total of about $86 billion lost as a direct result of the cyberattacks, “with companies incurring an average of $188,000 in losses.”23 Another study cited by a U.S. Secret Service representative to the House Committee on Homeland Security found that “average small to medium-sized businesses...will lose about $200,000 [per attack]. 80 percent of those companies, within 6 months, will go out of business.”24 These types of risks are especially damaging to small businesses that do not have the resources available to deal with the cyber threat, much less compensate the customers put at risk by the breach and recover their brand’s credibility.25 These reports show the incredibly damaging effect that cyberattacks can have on a country’s small business population, which has traditionally been the lifeblood of the American economy. The United States flourishes when there is significant innovation at the grassroots level; as small businesses do better, the economy generally tends to do better. “Small businesses are the driving forces behind further technological innovation as they produce about 13 times more patents per employee than other businesses.”26 As the risk of computer attacks increases, small businesses will suffer and the effect on the national economy will become more pronounced.

Target is not the only recent victim of significant cyberattacks. JPMorgan has recently been attacked by state-sponsored hackers from countries such as China and Iran. In June 2014, 83 million “names, addresses, and email addresses” of individuals and small businesses were stolen from the bank.27 In an effort to combat the attacks, JPMorgan has spent a considerable amount of money hiring ex-military cybersecurity specialists to evaluate and harden its

21 Ibid., 3.
25 77% of firms think that they are safe from cyber-attack, and 87% do not have a security policy in place. U.S. House, Protecting Small Businesses against Emerging and Complex Cyber-attacks, 2.
26 Ibid., 3.
systems. Sands Las Vegas Corporation, a company that runs many big-name casinos in Las Vegas, was also the victim of a severe attack. According to news sources, customer data was stolen and there was some amount of physical destruction as part of the attack.28 James Clapper, the Director of National Intelligence, has stated that the Iranian government was responsible for the attack.29 The popular ride-sharing app Uber was also attacked in 2014, resulting in the leak of 50,000 Uber drivers’ personal information. To compensate the drivers, Uber is providing them with a year of identity fraud service, but the company’s competitiveness may be severely impacted.30 At the beginning of 2015, it was announced that Premera Blue Cross, a large health service provider, was also compromised and the information for 11 million people was stolen.31 This news comes shortly after another large medical group, Anthem, was also broken into. For that specific case, it is still unknown how many records were taken, but Anthem had a customer base of over 69 million people.32 These large attacks illustrate the sheer amount of information that can be gained from these cyberattacks and why hacking groups find it worthwhile to go after these companies. These breaches of security cost the United States dearly, both monetarily and in terms of

competitiveness. In one report, McAfee estimates that there is a “$100 billion dollar annual loss to the U.S. economy and 508,000 U.S. jobs lost due to malicious cyber activity.”

How Cybersecurity Affects U.S. Competitiveness – China

One aspect of the impact that cybersecurity has on U.S. competitiveness is the economic costs associated with breaches in cybersecurity. As mentioned in the previous section, cyberattacks are extremely costly to the victim and can result in both physical and economic damage to a company. When the financial burden brought about by a cyberattack is too large for the company to justify trying to recover from, the business is shut down and the jobs it previously provided disappear. This destruction of small businesses not only carries the negative effects of adding to the unemployment population and lowering the number of jobs available in the United States, but it also destroys the innovation that the small business could have made had it not been the victim of a cyberattack. The lack of innovation by definition makes the United States relatively less competitive when compared to other countries, especially since the United States relies on being innovative for a large portion of its economy. A significant portion of the U.S. economy is largely service-based, and without innovative services that are able to effectively solve people’s problems, there would be no product to make the country more competitive.

Innovation has been a significant factor in U.S. global competitiveness. By creating intellectual property that meets the demands of consumers, the United States is able to grow its economy and continue to develop. One important threat to U.S. innovation is the threat posed by countries seeking to use technology to steal intellectual property, thus undermining U.S. innovation. In the words of a counterintelligence official, “trade secrets developed over

thousands of working hours by our brightest minds are stolen in a split second and transferred to our competitors.”[^34] Currently, the worst offender has been China[^35]. It has been estimated that “China accounts for 50 to 80 percent of [intellectual property] theft around the globe” which “costs the U.S. economy hundreds of billions of dollars a year and literally millions of jobs, dragging down our GDP and undermining our ability to innovate and prosper.”[^36] Such conflicts over cybersecurity issues have severely strained U.S.-China relations.[^37] A recent report from the computer security firm Akamai states that China is responsible for 41 percent of the world’s cyberattack traffic (as seen in Figure 4).


[^34]: U.S. Senate, The Cybersecurity Partnership between the Private Sector and Our Government, 8.


[^36]: Ibid., 2.

According to a very detailed report by Mandiant, China has put together a specially trained team of thousands of employees whose sole purpose is to break into foreign computers and steal intellectual property data. The group, called Unit 61398, is suspected to be headquartered in the building depicted in figure 5 and has stolen “hundreds of terabytes of data from at least 141 organizations.”  


Figure 6 is a map depicting the countries that have been stolen from and the number of times that information has been stolen from each country.

---

38 Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units,” 3.
Figure 6. Geographic location of APT1’s victims [and the number of attacks on each], in Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 22.

In the past, the Chinese government has denied all accusations of building a cyber army, but in a recent publication it revealed the existence of both military and government cyber forces. Many high level Chinese agencies, such as the Ministry of Public Security (similar to the U.S. FBI) and the Ministry of State Security (similar to the U.S. CIA) have developed extensive cyber capabilities and employ thousands of hackers.39 Most U.S. scholars and intelligence community members already knew that this was the case, but the Chinese government’s shift in position could be an important signal of its commitment to use their cyber forces in a more open way in the future.40 While these forces gather a great deal of intellectual property and information from competitive U.S. businesses, they also target U.S. military sources to gain access to advanced technology. For example, using information obtained through cyber espionage, China was able to construct an advanced fighter jet called

---

the J-20 stealth airplane, an airplane that is remarkably similar to the new U.S. F-35. According to experts reporting to the House Committee on Homeland Security, the new Chinese plane was “years ahead of what all the experts predicted that China was able to do on its own.”\(^{41}\) In an effort to combat the theft of U.S. intellectual property and the continued attacks on critical systems and infrastructure, President Barack Obama issued an executive order allowing the government to place sanctions on any country or individual who participates in or supports these attacks or related activities.\(^{42}\)

Despite all of the U.S. criticism of China’s methods regarding cybersecurity, some of the U.S. methods have rightfully angered China as well. One of China’s biggest objections is the United States’ use of the National Security Agency (NSA) to conduct domestic and international espionage. The NSA has been found performing dragnet data collection and using newfound encryption and delivery processes to send bugged or back-doored hardware and software to other countries with the intention of monitoring them. China has responded by implementing many restrictions in order to deal with these concerns. The first is to remove most U.S. tech supplies from government procurement lists, to which U.S. manufacturers such as Cisco have reacted negatively.\(^{43}\) However, despite the Chinese government’s willingness to dismiss U.S.-made products altogether, the action does not put regulations on individual businesses or lower levels of government. The second response of the Chinese government is to roll data collection under the umbrella of counterterrorism law, similar to what the NSA has


done. The most recent draft of a new counterterrorism law floating around for the past few months includes provisions that would require businesses and banks to give up private encryption keys and store all data in China so that it could be accessed for monitoring for terrorist threats. This requirement includes a provision that states that banks may not use foreign software and are included in the requirement to provide encryption keys to the Chinese government. This act has posed significant privacy issues for many U.S. companies doing business in China and has created a type of hostile security environment in the mainland. These issues will continue to provide a challenge to the U.S. business community, not only due to new threats of cyber espionage by having to turn over proprietary encryption keys, but also the increased restrictions placed on the sale of foreign technologies inside of China.

---


Overview of Current U.S. Policy

Figure 7. Evolution of national strategies related to cybersecurity, in U.S. Senate, The Cybersecurity Partnership between the Private Sector and Our Government, 60.

Due to the novelty of cyberspace, uncertainty of how large its role would be in the future, and concern for the preservation of civil liberties, there was not much significant policy action on cyber issues before 2001. However, as shown in figure 7, there was a growing concern after 9/11 that technology could provide the answer to preventing another major terrorist attack. In an effort to prevent additional attacks, agencies such as the NSA and the FBI were expanded and given greater legal authority to conduct surveillance and investigations. Since that time, several initiatives by many different government organizations have been enacted, and most government agencies now have some sort of cyber branch.

The FBI has largely focused on high-level threats like botnets (a large collection of remote-controlled zombie computers used for malicious purposes) and state-sponsored
attacks.\textsuperscript{47} It has recently expanded efforts to include responding to major cyber incidents, as well as working with interagency communication groups to foster the transmission of useful information from one government agency to another.\textsuperscript{48} The Secret Service has also been a major player in cybersecurity cases due to a congressional mandate in 2001 to “prevent, detect, and investigate” various types of cybercrime in the United States.\textsuperscript{49} The CIA has very recently begun to make changes to its basic structure in order to accommodate a larger focus on cybersecurity issues. Many people believe that, due to each agency’s tendency to form its own cybersecurity group, there will be a more pronounced problem regarding inter-agency information sharing in the future regarding cybersecurity.\textsuperscript{50} The Department of Homeland Security has also been heavily involved in combating cyber threats and is home to the National Cybersecurity and Communications Integration Center (NCCIC), which provides constant monitoring and incident response for the U.S. government and law enforcement.\textsuperscript{51} The DHS is “responsible for coordinating the [federal government’s] response to significant cyber or physical incidents affecting critical infrastructure,”\textsuperscript{52} but there is still a lot of room for improvement in the realm of inter-agency cooperation.\textsuperscript{53} Some of the difficulties of inter-agency cooperation stem from the traditional agency culture that frowns upon having to work with other agencies to solve a problem, especially when that problem involves questions of jurisdiction. However, the greatest difficulty to cooperation is the mutual incompatibility of

\begin{footnotesize}
\begin{enumerate}
\item Ibid., 21.
\item Ibid., 8.
\item Ibid.
\end{enumerate}
\end{footnotesize}
agency computer systems; each agency’s network is separately developed and maintained, which makes the mass integration and sharing of information technically impossible. While this separation is an effective security measure in itself, the ability to cooperate in a timely manner could be key to investigating significant trends and preventing attacks in the future.

Cooperation between the public and private sector has been stressed as a crucial aspect of U.S. cyber response. The Cybersecurity Act of 2013 provides instructions to set practical standards with the National Institute of Standards and Technologies (NIST, a government organization who helps regulate national standards, including those relating to computer security) and help spread them to both government agencies and private companies over time and through voluntary means.\(^{54}\) In addition, President Obama signed an executive order directing agencies to focus a greater deal of effort on the sharing of information while protecting the privacy of U.S. citizens, which is a difficult balance to maintain.\(^{55}\) Such sharing of information, especially private companies (like internet service providers) sharing information with the federal government, has created quite a stir among privacy advocates who say that the measures taken to protect American privacy are not strong enough and are open to abuse. Activists cite the mass data gathering techniques used the NSA with no meaningful oversight\(^{56}\), as well as the great deal of government secrecy surrounding issues of cybersecurity, to justify their argument that privacy rights are being infringed upon.\(^{57}\) Most recently, congress has been discussing the Cybersecurity Information Sharing Act of 2014, which is supposed to “facilitate sharing of information between private companies and government agencies” by developing procedures for open sharing of unclassified threats and the restricted sharing of

\(^{54}\) U.S. Senate, Cybersecurity Act of 2013, 6.  
\(^{56}\) U.S. House, DHS Cybersecurity, 59.  
\(^{57}\) Ibid., 60.
classified threats.\textsuperscript{58} However, privacy advocates says that the language used in the bill is too broad and incorporates the sharing of information on other physical crimes (such as murder or theft) in a bill that is supposed to only be dedicated to the prevention of cyberattacks.\textsuperscript{59}

\textit{Policy Proposals}

Though combating a seemingly omnipresent threat capable of inflicting damage on nearly and remote target is difficult, it is not impossible. To increase the strength of U.S. cybersecurity and defend against future attacks, I recommend that the government focus on providing cybersecurity tools and information to the public, promote the implementation of secure forms of communication and purchasing, as well as devote more resources to the research and development of both offensive and defensive cyber tools. The United States needs to take a firm stance against cyber crime and back up rhetoric with specific and effective counter procedures.

In order to more effectively address the cybersecurity concerns of the nation, a great deal of effort must be focused on the grassroots level through education and government partnership to prevent and mitigate potential cyberattacks. “85 percent of the assets that are engaged in the world of cyber are in the hands of private entities,” which stresses the importance of securing the national network as a whole rather than just targets significant to the national government.\textsuperscript{60} The federal government agencies need to share more information regarding cyber threats with the private companies that are most at risk from the attacks. The Chair of the House Intelligence Committee has said that, “according to intelligence officials,

\textsuperscript{60} U.S. House, \textit{Protecting Your Personal Data}, 8.
allowing the government to share classified information with private companies could stop up to 90 percent of cyberattacks on U.S. networks.\textsuperscript{61} Through the sharing of information, businesses would be better equipped to handle potential cyber threats and would be more aware of the risks that they face. Currently, most small businesses do not have any sort of protections against cyberattacks, which could be changed by government encouragement to develop a set of company-wide standards to ensure data security.\textsuperscript{62} In addition, government agencies providing assistance while investigating a cyberattack need to provide more useful feedback and investigation results to the businesses that were affected in the breach so that the company can strengthen their systems and prevent a similar attack from happening in the future.

The U.S. government also needs to better maintain its public image when it comes to cybersecurity organizations and branches. The government should seek to further consolidate cyber threat entities into one, coherent body capable of responding to threats in the shortest amount of time possible. Similar to the 9-11 emergency phone service in America, there needs to be an organization set up to efficiently handle reports of cyberattacks, route them to the most suitable agency (whether it be a public or private agency), and the follow up on the threat to make sure that it was handled properly. This would streamline the reporting process and allow for individuals and businesses to receive more timely aid in the event of a serious attack. Related to the need for a single public face of government cyber threat response is the need of public relations efforts to educate both businesses and individuals on proper cyber-

\textsuperscript{61} U.S. Senate, \textit{The Cybersecurity Partnership between the Private Sector and Our Government}, 8.

\textsuperscript{62} Cyber Security Alliance and Symantec interviewed more than 1,000 businesses with fewer than 250 employees and found that 90% did not have an IT manager focused on IT issues, 87% did not have a security policy, 63% did not provide cybersecurity training to employees, and 83% did not have an internal password regulation system. U.S. House, \textit{Protecting Small Businesses against Emerging and Complex Cyber-attacks}, 22.
response procedures and practices, similar to how businesses conduct fire drills to make sure employees know how to handle a potential fire. For the cyber-response needs of individuals, internet service providers could be used as a middleman between government agencies and the individual consumer, whereas small businesses would have a more direct access to government aid and large corporations could contact more specialized units for a quicker response. As the size of the company grows larger, the importance of handling the threat in a timely manner to identify the problem and minimize damages increases. However, in order for individuals and private businesses to effectively diagnose a cyberattack, they must receive some form of specialized cybersecurity training. The government must work with private companies to provide individuals with a basic understanding and education of cybersecurity and proper response procedures. Public education programs sponsored by the government in addition to information provided by internet service providers could help people gain easier access to the information they need to learn how to secure themselves or their businesses from a cyberattack. In addition, the curriculum of computer technology classes in public schools could be altered to focus less on the fundamentals of computing that children tend to learn in elementary school and more toward safe computer practices and how to identify report problems. Computer technology will only become more prevalent as time goes on, and having a population that is educated in the basics of cybersecurity will be essential to the future national security of the United States.

In order to prevent the overwhelming costs of data breaches and leaked financial and personal information, the United States government needs to mandate the widespread adoption of the “Chip and PIN” payment technologies. Currently, the United States uses the “swipe and signature” method of transactions, which has made the United States comparatively weak when it comes to protecting consumer credit card information. Therefore,
the United States has been the focus of a greater number of attacks compared to other countries where “Chip and PIN” technology is already widespread and, in most cases, required. “The United States is the last of the G20 nations to move to more secure chip-based cards,” which has compromised the security gains of the new technology worldwide.\textsuperscript{63} This technology uses a small chip embedded in a credit or debit card, paired with a PIN number that makes the credit card information useless without both the physical card and the correct PIN number. Some card companies have started to adopt chip technology, but adoption has not been mandated and is currently not widespread, especially due to the financial cost of purchasing new hardware to accept the new payment standard. It has been estimated that it would cost retailers in the United States approximately $30 billion to replace the necessary hardware, implement the software, and train employees on the new system.\textsuperscript{64} This cost has thus far been too great for retailers to accept, but the government should take action to subsidize the adoption of the new technology in order to bring the United States up to speed with the majority of other countries around the world. President Obama has made efforts to promote the adoption of the new more secure payment technology by government agencies, but has not yet expanded the promotion to private companies.\textsuperscript{65} Other countries who have successfully implemented the standard, such as the United Kingdom, have had extensive government involvement in the transition process. The United States should study these countries’ methods and develop a plan to transition to more secure forms of payment and transactions.

\textsuperscript{64} U.S. House, Protecting Your Personal Data, 51.
In addition to adopting new payment standards, the U.S. government needs to provide a shining example of what it means to be adequately protected from cyberattacks. While it is impossible to guarantee that any piece of technology cannot be attacked, practices such as using the most up-to-date software, using stable operating systems, and strengthening government encryption of sensitive data can provide significant protection against known bugs and vulnerabilities. Currently, many government computer systems still run on Windows XP, which has been out of production and has stopped being supported by Microsoft. Microsoft is attempting to mitigate the issue by offering free upgrades to its latest operating system, Windows 10 coming the summer of 2015, but the government needs to take the necessary steps to prepare for the transition to more secure operating systems and software overall. Once the government is able to implement the best practices, it can help others do the same. There are many areas where private businesses fall under some sort of government regulation, and the government can use inspection times as an opportunity to assess the security of each private business and provide guidance for improvement. These checks and prescriptions would not be required or mandated by any group, but simply provided to those companies who wish to use them to strengthen their resistance to cyber threats.

Finally, the United States must not only continuously research and develop new means of cyber defense, but also develop the additional offensive cyber tools necessary for the protection of American interests in cyberspace. These types of offensive tools have been used by other countries for their own gain in the past. For example, China has recently been caught using a new offensive cyber tool called the “Great Cannon” to selectively censor websites who

---

seek to undermine the Chinese government’s policies by proving access to foreign media.67 According to the New York Times’ report, U.S. agencies like the NSA have used similar tools in the past. The development of these tools is essential to protecting the United States from future cyber threats as well as responding to attacks.

Conclusion

Cybersecurity entails the protection of vital systems and information from the destruction or misuse by those who would abuse the data for selfish purposes. As technology becomes more prevalent, the risk to all those connected to global networks increases and necessitates the adoption of a set of best practices designed to minimize the risk of becoming the victim of a cyberattack. As the government takes a more active role in educating its citizens, strengthening its own systems, and adopting secure technologies, the future risk of attack will decrease and the United States can focus more attention on other matters of importance without the worry that U.S. innovations and technologies will be compromised. Without the financial burden caused by the misuse of personal information or the dangers presented to competition through cyber espionage, businesses in the United States can feel more confident that their information is secured and that they can continue to pursue innovations that contribute to the overall state of the national economy. There is a great deal of effort still required to fully secure U.S. networks and address the growing prevalence of damaging cyberattacks, but the benefits far outweigh the costs. Investment in cybersecurity is an investment in future global competitiveness of the United States.

---

BIBLIOGRAPHY


Ebert, Hannes and Time Maurer. “Contested cyberspace and rising powers.” *Third World Quarterly* 34, no. 6 (2013): 1054-1074.


