# Cybersecurity and United States Policy Issues

Cristina Berriz
Peace, War and Defense Program
University of North Carolina at Chapel Hill
Chapel Hill, NC 27514
cberriz@gmail.com

**Keywords:** Cyber, Cybersecurity, Intelligence, Cyberattack, Cyberspace, Cybercrime, CISPA, Department of Homeland Security, Department of Defense, National Security, Counterterrorism, ECTF, Information-sharing

## Abstract

In a time when nearly everything is done through computers and the internet, our world is faced with serious security threats in the cyber-world. Specifically, in the United States, the problem of cybersecurity is not being given proper attention or funding and it is putting our nation's intelligence and personal information at a serious security risk. Congress cannot come to an agreement on legislation, federal spending has been given, but not in significant amounts, and there is a serious lack of communication among all parties. These are all issues than can be directly addressed and fixed quite simply—cybersecurity is not a bi-partisan issue, it is something that affects us all, and our government needs to tackle it head on to protect our national against a serious international threat.

## Introduction

When picturing modern warfare, images of RPGs and assault rifles come to mind, but very few people imagine a single person in front of a computer taking down a city in less than a day. One of the biggest national and international security threats facing our world today are the cyber attacks that have the ability to shut down power grids, obtain government secrets, and steal intellectual property. A strategic cyber attack can literally shut our country down—we wouldn't have access to banks or emergency operators, electricity to cool or heat our homes and keep our food refrigerated would be gone, communications between government agencies would be limited. However, despite all these blatant issues that could possibly arise from a cyberattack, major improvements are not progressively being made in securing our cyber networks from our adversaries. Congress can't agree on the right balance between securing our networks and securing our privacy, organizations won't communicate with one another about potential cyberattacks coming their way, and not enough funding is being allocated for improving our defense mechanisms against future cyberattacks. If our government and private organizations can communicate, agree, and significantly fund cyber-defense, the security of our nation would be greatly improved for future years to come.

## Legislative and Executive Efforts

In 2011, Congress got to serious work on passing legislation that would protect our intelligence on the cyber level by helping companies defend themselves from foreign hackers.

This act, the Cyber Intelligence Sharing and Protection Act (CISPA), was presented as an amendment to the National Security Act of 1947, which obviously did not have provisions for cybersecurity issues when made. CISPA clearly defines a cyber threat as an "effort to degrade, disrupt, or destroy [a] system or network" or the "theft or misappropriation of private or government information, intellectual property, or personally identifiable information," (U.S. H.R. 624 2011). Many opponents to this bill, privacy advocates and civil liberties groups, were concerned that the bill would expose private online records to the federal government, such as health or credit records, giving the National Security Agency the ability to spy on U.S. citizens (Flaherty 2013). However, amendments were added to the bill the allowed lawsuits to be brought against the government in the case of any violations of the government's use of this private information (U.S. H.R. 3523 2012). Although there is definite opposition to this bill, clear in the fact that it's 2014 and still it has not been passed through the Senate, businesses are struggling on a daily basis to defend themselves against attacks from hackers in China, Russia, and Eastern Europe (Flaherty 2013). Everyday banks are fighting away foreign intrusions, newspapers servers are being penetrated, and businesses are hoping that their information hasn't been stolen and taken advantage of. While the privacy advocates and civil liberty groups may fear their private information being stolen, lobbyists from every industry are begging for this bill to be passed so that their companies are protected. In her article on the CISPA bill, Anne Flaherty acknowledges that there has not yet been a cyberattack that has severely hurt the U.S. economy or infrastructure, but until we secure our networks against it, it's only a matter of time. As a supporter and leader of the bill, Rep. Mike Rogers says, the bill strikes "that right balance between our privacy, civil liberties and stopping bad guys in their tracks from ruining what is one-sixth of the U.S. economy" (Flaherty 2013).

While President Obama has identified that the "cyber threat is one of the most serious economic and national security challenges we face as a nation," not many strides are being made towards improving our security ("Foreign Policy Cyber Security" 2014). He acknowledges that in order for our economy to prosper nowadays, we must rely heavily on cybersecurity and thus do everything in our power to protect against intruders. The White House has a twofold strategy aimed at improving our nation's cybersecurity. The two main facets of this strategy are to "help improve our resilience to cyber incidents" and "reduce the cyber threat" we face everyday. These two strategies include strengthening our digital infrastructure against penetration from adversaries, constantly advancing our defense techniques with the sophisticated cyber threats, and responding and recovering quickly from cyber attacks, among other things ("Foreign Policy Cyber Security" 2014). The White House wants to work with our allies on establishing some international norms about acceptable behavior in cyberspace and strengthen the actual law enforcement against cybercrimes. The Department of Homeland Security has various measures they take in order to secure our cyberspace which include releasing actionable cyber alerts, investigating and arrest cyber criminals, and educating the American people about how to prevent cyberattacks by staying safe online ("Cybersecurity Overview" 2014). The Secret Service has a unit specifically designed to focus on cyberattacks and cyber criminals called the Electronic Crimes Task Force (ECTF), ("Combat Cyber Crime" 2014). These ECTFs deal with issues of cyber intrusions, bank fraud, data breaches, and other various cyber crimes, such as the theft of hundreds of millions of credit card numbers. In just 2011, the Department of Homeland Security charged 72 individuals for participating in sexual abuse of children by creating and distributing graphic images and videos of these children online ("Combat Cyber Crime" 2014). While it cannot be said that our government is not taking any action towards dealing with the

cyberattacks on our nation's systems, our government definitely needs to be taking a defensive approach when focusing on cyber warfare.

Over the history of cyber attacks in the United States, it seems that the government has not learned from previous attacks and made efforts to strengthen our systems, but rather let the same types of attacks happen once again. In 1997, the Department of Defense organized a planned, tester cyberattack called "Eligible Receiver" that hacked into the Pentagon computer systems ("Cyberwar! The Warnings" 2003). The DOD was very specific in that the hackers should only use computer equipment and software that was easily and publicly available so that they were not given any special advantages. In this trial run hacking of the Pentagon, they were able to infiltrate the computer systems and take control of the Pacific command center computers. Through this, they had control of power grids and emergency operating systems in nine major cities. Just one year late, in March of 1998, a highly classified incident, codenamed "Moonlight Maze," U.S. officials realized that computer systems throughout many government organizations, universities, and research labs were being routinely probed for information ("Cyberwar! The Warnings" 2003). This went on for nearly two years before anyone noticed and during that time, the hackers were able to steal thousands of files that including maps of military installations and hardware designs and troop configurations. Although the perpetrator has never been found and the investigation is ongoing, they did trace the computer back to the former Soviet Union, but Russia denied any involvement with the activities. What makes "Moonlight Maze" such an important attack is that it happened only on year after "Eligible Receiver." Just one year before, the Pentagon realized they had holes in their security system through their exercise, but they didn't strengthen those holes securely enough because someone was able to infiltrate the servers and steal important information from our government. Early on, the government showed an incapability of learning from past attacks and strengthening the system against future attacks. In the summer of 2011, just months before the 9/11 attacks, a city in California noticed a pattern of intrusions into their computer systems where hackers were gaining information about government offices, cities' utilities, and emergency systems. This town, Mountain View, was the first to report the intrusions and the FBI soon found similar searches through other cities in the U.S. and discovered they were originating in the Middle East and South Asia. While information about cities is something our government wouldn't necessarily want other countries to have access to, these probes didn't hold any real significance until September 11, 2001, when U.S. intelligence officials discovered U.S. infrastructure surveillance on computers they had seized from Al Qaeda operatives ("Cyberwar! The Warnings" 2003). Although there were no concrete ties between "Mountain View" and Al Qaeda, the situations were very coincidental and got the attention of intelligence organizations. They realized how significant these cyberattacks could be—they weren't just gathering arbitrary infrastructural logistics, they were possibly planning out future terrorist attacks.

**Communication**

In Martin Libicki's article, "Don't Buy the Cyberhype," he argues that there have been no major cyberattacks that have significantly affected individuals' lives, but the more one looks into the subject of cyberattacks, it's easy to see this isn't necessarily true (Libicki 2013). If a hacker breaks into businesses' records and steals credit card information or personal records, those lives are affected. If banks' security systems are infiltrated, millions upon millions of dollars are at risk and for some people, that's their next paycheck, their next meal. It can be argued that these

aren't true attacks on the United States, but individuals are absolutely feeling the effects of cyberattacks and as Libicki notes, we need to take steps to prevent the attacks from even happening. One big issue that Libicki touches on is the need to communicate intelligence information between organizations and businesses (Libicki 2013). Not only do we need to be giving potential victims access to the intelligence we've acquired, whether "we" is the government or individual firms, but we need to be sharing software we've acquired as well. If a vulnerability or flaw in software has been discovered and we know how to fix that issue, this needs to be shared across our country so that as a whole, our cyber networks are more secure. In Baltimore, Maryland, the Department of Labor was recently on the receiving end of a cyberattack. When an email was sent out to the department, an employee opened up the attachment an instantly ransomware attacked the computer and took all of the information. The hackers tried to exploit money out of the Department of Labor to get the information back, but the IT department responded quickly, shut down the computer system, and backed up information from an external drive ("Local Government Agencies" 2014). The main takeaway from this article was that agencies and businesses need to communicate with each other and immediately let them know that there are emails being sent out with suspicious attachments that could harm their businesses. In the case of the Maryland Department of Labor, they were fortunate enough to have an IT department that was quick to respond, but if a company does not have a backup drive, they are forced to either lose all their information, or pay the money to the hackers.

**Federal Spending**

When Adam Crain, the owner of a small tech firm in North Carolina, tried hacking into the power companies' computer networks, he was surprised to find that he had little to no trouble penetrating their servers. He found he was able to shut down power grids and it didn't require much effort ("Power Grid Shockingly Vulnerable" 2014). The power companies were fortunate that this man immediately contacted the utility security officials and alerted them to the gaping hole in their security software, but a hacker would take advantage of that and potentially shut down the power, devastating local towns. In this editorial, it's brought to attention that the Federal Energy Regulatory Commission did a study that showed that if "only nine of the nation's 55,000 transmission substations" were shut down, power could potentially be lost around the country for more than a month ("Power Grid Shockingly Vulnerable" 2014). It's noted that this kind of attack would be more detrimental to our country and our economy than even 9/11. It depicts a situation in which it's the death of summer or winter and we have no electricity, no electronic communication, no way of getting money—we would be at a complete loss of how to go on with our daily lives. This editorial touches upon a very important factor that not many people realize: 650 *billion* dollars are spent each year on our defense budget, but only 447 million dollars are spent towards the military cyberspace operations that protect the information in our Department of Defense (Walker 2014). It's interesting that an issue our president calls one of the "most serious economic and national security challenges" our country currently has, receives less than 1% of the budget that our military defense receives. If it's such a serious issue and our economic prosperity *depends* on cybersecurity, why is our government not devoting more time and funding towards it?

**Conclusion**

It seems as though every other day we are inputting our addresses, credit card numbers, or our social security numbers into some website. Everyday our banks are moving around our money. Our businesses and agencies are filing away our most personal information. Our military and intelligence organizations are strategizing and communicating. And while all of this is happening, our government is doing very little to protect this valuable information from the hands of our enemies, the bad guys. At this very moment, terrorist organizations across the world could be gathering the locations of our troops abroad, learning the infrastructure of a city they want to take down, and garnering intelligence information that will help them along the way. If we want to protect our government, our country, and our people, we need to take definitive steps towards preventing these cyberattacks. First and foremost, we need to promote information-sharing across organizations. When the government gets ahold of news that a cyberattack is under way, they need to immediately alert all other government organizations and assess whether this could affect individuals or businesses. If it is found that these cyberattacks could affect us on a daily basis, the information must be passed on. Second, when security breaches are found within our systems and servers, we need to alert the proper authorities and enhance our security software. Once we have enhanced this security software, we need to make it widely available to other government organizations and if appropriate, once again, pass it on to individuals and businesses. Information-sharing is probably the most important and effective step we can take as a country in preventing cyberattacks from enemies. Next, our congressmen need to come to an agreement with the Cyber Intelligence Sharing and Protection Act. While it is incredibly important to protect our privacy rights, it could be argued that protecting our country from cyberterrorism is a more pressing need. There are now provisions in the bill that will allow action to be taken against the government if they are found to be misusing personal information and the businesses absolutely need help protecting their computer systems from the high-tech attacks coming from hackers across the country. More often than not, arguments between the House and Senate are bipartisan issues, but the congressmen need to realize that every minute wasted arguing is another minute given to a hacker. Lastly, our federal government needs to give cybersecurity the funding it needs and deserves. We need to be developing the highest level of technology when it comes to securing our computer systems and in order to do that, we need to hire the best of the best, which will cost us money. If the defense budget gave up 1.5% of its budget, just 10 billion dollars, the budget of cybersecurity would raise by over 2000%. When it's put into that perspective, it seems ridiculous that are government is not prioritizing one of the biggest issues of national security facing our nation today. If our government and nation is able to come to an agreement on how to best tackle cybersecurity in a legislative manner, effectively communicate techniques and attack information between one another, and give cybersecurity the proper funding it needs, our country will strengthen its computer systems and national security tenfold and push the United States further up as a secure world power.

**References**

"Bill Status Update - H.R. 3523." *Permanent Select Committee on Intelligence*. U.S. House of Representatives, 16 Apr. 2012. Web. 21 Apr. 2014.

"Combat Cyber Crime." *Department of Homeland Security*. Department of Homeland Security, April 24, 2003. Web. 21 Apr. 2014.

"Cybersecurity Overview." *Department of Homeland Security*. Department of Homeland Security, n.d. Web. 21 Apr. 2014.

"Cyberwar! The Warnings." *PBS*. Frontline, n.d. Web. 21 Apr. 2014. <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/>.

Flaherty, Anne. "House Passes Pro-Business Cybersecurity Bill." *Claims Journal News*. Claims Journal, 19 Apr. 2013. Web. 21 Apr. 2014.

"Foreign Policy Cyber Security." *The White House*. The White House, n.d. Web. 21 Apr. 2014.

Libicki, Martin. "Don't Buy the Cyberhype." *Foreign Affairs*. Foreign Affairs, 14 Aug. 2013. Web. 22 Apr. 2014. <http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype>.

"Local Government Agencies Targeted In Cyber Attackss." *WBFF Fox Baltimore*. Fox, 21 Apr. 2014. Web. 21 Apr. 2014. <http://www.foxbaltimore.com/news/features/top-stories/stories/local-government-agencies-targeted-cyber-attacks-27371.shtml#.U1XwO61dXRt>.

"Power Grid Shockingly Vulnerable to Cyberterrorism." *The News Tribune*. The News Tribune, 21 Apr. 2014. Web. 22 Apr. 2014. <http://www.thenewstribune.com/2014/04/21/3158485/power-grid-shockingly-vulnerable.html?sp=/99/447/>.

United States of America. House of Representatives. *H.R. 624 - Cyber Intelligence Sharing and Protection Act*. N.p.: n.p., n.d. Print.

http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/CISPAPassedApril2013.pdf

Walker, Richard W. "Budget Bill Boosts Cybersecurity Spending." *InformationWeek - Government*. InformationWeek, 1 Jan. 2014. Web. 22 Apr. 2014. <http://www.informationweek.com/government/cybersecurity/budget-bill-boosts-cybersecurity-spending/d/d-id/1113494>.