Interested in learning more about security?

SANS Institute InfoSec Reading Room

Cyberspace: America's New Battleground

There is a global war going on. It is a war being waged not with bombs and missiles but with bytes and keystrokes. As with other global wars, like World War II and the Global War on Terror, the United States was slow at first to respond to the threat, but then quickly ramped up and began devoting resources to prevent future attacks and launch counterstrikes. Also, as with other wars, the protective measures proposed and instituted at home have raised some thorny legal and privacy issues. This paper describes the techni...

Cyberspace: America's New Battleground

GIAC (GSEC) Gold Certification

Author: Maxwell Chi, Maxwell.chi@sbcglobal.net

Advisor: Richard Carbone

Submitted: November 14, 2014

Abstract

There is a global war going on. It is a war being waged not with bombs and missiles but with bytes and keystrokes. As with other global wars, like World War II and the Global War on Terror, the United States was slow at first to respond to the threat, but then quickly ramped up and began devoting resources to prevent future attacks and launch counterstrikes. Also, as with other wars, the protective measures proposed and instituted at home have raised some thorny legal and privacy issues. This paper describes the technical and legal issues associated with cyber warfare. It gives a brief history of global cyber war and describes the defensive and offensive measures currently being undertaken by the U.S. government to prosecute this war. It then summarizes some of the legal and privacy issues and offers recommendations for how these might be addressed. It also offers some suggestions for addressing cyber security deficiencies in the private sector.

1. Introduction

In 2010, Nick Percoco, head of the cyber security team at IT security service provider TrustWave Holdings Inc., was called out to the headquarters of a leading U.S. defense contractor to investigate some anomalies (Taylor, 2011). The anomalies seemed innocent at first. A few employees had reported peculiar behavior by their PCs when they clicked on an innocuous-looking email attachment they had received.

The users whose PCs were acting strangely had all received an email that appeared to come from a human resources manager in the company. The email included a legitimate signature and urged the recipients to click on a PDF attachment. The recipients included senior executives at the company who were familiar with the HR manager and thought little about double-clicking the attachment that appeared to come from this person.

When users opened the attachment, the PDF file opened, quickly closed, and then a fictitious letter was displayed about a new hire at the company. Behind the scenes, however, a small executable file was copying the contents of the users' 'My Documents' directories, and transmitting them as compressed files to a foreign IP address. The Trustwave and federal law enforcement investigators soon concluded they were dealing with a case of foreign cyber espionage.

There was sound basis for this conclusion. At around the same time period as this incident, defense contractor Lockheed Martin announced that it had been the victim of a "significant and tenacious" Internet attack, and Internet security company McAfee reported a massive cyber espionage operation, called SHADY RAT. McAfee said the operation had penetrated over 70 government and other organizations in the U.S. and other countries worldwide over the previous five years and resulted in the theft of "everything from military secrets to industrial designs" (Menn, 2011).

The incident that Trustwave was investigating was more isolated. Rather than a coordinated series of attacks, this was an attempt to steal as much data as possible in one sweep. Said Percoco, "There was no functionality in the payload to wake up periodically and send those files out again. This was more them trying to just smash the windows in the building and run off with as much as they could carry" (Taylor, 2011). Furthermore, not all users kept files in their 'My Documents' folders, and the total amount of data stolen was estimated to be more in the megabytes than terabytes range (Taylor, 2011).

Although the source of the attack was never identified, Percoco and his colleagues helped the company institute measures to prevent future break-ins. The company at the time lacked intrusion detection systems that monitored network activity and alerted suspicious behavior. Furthermore, the company was advised to put critical employees, such as senior executives, into a group for special monitoring because they represented high-profile targets. Percoco also pointed out the importance of protecting company documents even if they are not sensitive, as such documents may still be of value to a competitor or foreign country.

The preceding example illustrates that cyber-attacks in today's world can originate from various sources, and that they are often hard to detect and prevent. But organizations can take measures to both protect themselves and limit the damage.

This paper is intended to provide background of the current state of global cyber warfare. It will give a brief history of cyber warfare and describe a few notable incidents. It will then summarize the defensive and offensive measures being taken by the United States to protect its electronic assets and prevent future attacks. Finally, it will provide some recommendations for addressing the legal and privacy concerns associated with these measures and suggestions for improving cyber security in private companies.

2. History of Cyber Warfare

Cyber warfare dates back to well before the Internet. In 1982, a Soviet gas pipeline in Siberia blew up; the biggest non-nuclear explosion in recorded history. The resulting fire could be seen from space. According to a book by Thomas C. Reed, a former secretary of the Air Force and member of the National Security Council, the explosion was the direct result of a CIA plot to undermine the Soviet economy (Loney, 2004). The CIA tricked the Soviet Union into acquiring software with built-in flaws and installing it in the controls for its Siberian pipeline, which the country was using to export natural gas to Western Europe. Reed wrote:

> "the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, … to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds."

> "While there were no physical casualties from the pipeline explosion, there was significant damage to the Soviet economy. Its ultimate bankruptcy, not a bloody battle or

> nuclear exchange, is what brought the Cold War to an end. In time the Soviets came to understand that they had been stealing bogus technology, but now what were they to do? … They had no way of knowing which equipment was sound, which was bogus. All was suspect, which was the intended endgame for the operation." (Loney, 2004)

2.1 The Internet poses a new cyber security threat

With the advent of the Internet, cyber-attacks could be conducted remotely, often from thousands of miles away, without requiring physical access to the targeted system. The global information security community lost no time in changing strategies to incorporate this new capability. Internet-based cyber breaches and discussions about Internet security began almost at the same time as the Internet itself.

In 1997, the Department of Defense (DoD) initiated an internal penetration exercise named Eligible Receiver, in which a Red Team from the National Security Agency (NSA) attempted to penetrate systems at the Pentagon, using only publicly available computer equipment and software. Public reports indicate that the team was able to access and assume control over DoD command center computers, power grids, and emergency networks in nine American cities (Hildreth, 2001).

One of the most well-known and extensive cyber security incidents against the U.S. started in 1998 and went on for about two years. Attackers systematically gained access to DoD computers and made off with large amounts of sensitive, but unclassified, data. The culprits also broke into unclassified information systems at the Department of Energy, NASA, and many universities and defense contractors.

An investigation led by the FBI, code-named Moonlight Maze, found evidence that suggested a Russian intelligence-gathering operation. For example, some of the attacks were traced to Internet servers near Moscow, and the attacks tended to occur on weekdays Moscow time, but not on Russian holidays.

Because of the incident, the DoD purchased new encryption software, firewalls, and intrusion detection equipment. It also redesigned its unclassified network to route all traffic through eight main gateways in order to make the network easier to monitor and eliminate the numerous backdoors that provided access (Drogin, 1999).

2.1.1 But some managers still had a 'cavalier attitude' toward cyber security

From 2003 to 2006, a series of carefully orchestrated penetrations was conducted against unclassified information systems at Sandia National Laboratories, Lockheed Martin, NASA, Redstone Arsenal, and Fort Huachuca, among others (Wegilant, n.d.). Dubbed Titan Rain by the U.S. government, this series of attacks compromised hundreds of computer networks and resulted in the massive theft of sensitive information. Many now believe the attackers were located in China and supported by the government there.

The attacks were discovered largely through the efforts of a Sandia employee named Shawn Carpenter. Carpenter investigated the breaches at Sandia and other agencies and noticed patterns that indicated a single group conducted the intrusions.

To indicate the attitude at Sandia at the time, when Carpenter reported his discoveries to his superiors, he was directed to drop his investigation and focus on attending to the Sandia computers. When Carpenter instead began sharing his findings with the FBI and U.S. Army, Sandia terminated his employment.

During his termination hearing, according to Carpenter, Sandia's chief of counterintelligence yelled, "You're lucky you have such understanding management... if you worked for me, I would decapitate you! There would at least be blood all over the office!" (Vijayan, 2007).

In a later lawsuit, a jury awarded Carpenter nearly $4.7 million in compensatory and punitive damages. The jury forewoman said jurors were upset by the "reckless behavior on the part of Sandia to not have adequate policies in place for employees about hacking, and the cavalier attitude about national security and global security" (Wikipedia, 2014).

2.2 Cyber warfare ascends to new heights

Throughout the early 2000s, cyber-attacks increasingly became used as an instrument of political power and protest. Two notable examples include Estonia in 2007 and Russia-Georgia in 2008.

2.2.1 Estonia, 2007

The first large-scale cyber assault on a country's infrastructure occurred April 2007 in the formerly Soviet-occupied state of Estonia. The focus of the incident was a Soviet-era statue in Estonia's capital which memorialized fallen Red Army soldiers in World War II. After Estonian officials decided to move the statue out of the city center to a military cemetery, two days of violent protests and rioting by Russian nationals in Estonia ensued.

As the rioting subsided, a cyber-attack on Estonia's information infrastructure began. Cyber attackers launched a distributed denial of service (DDoS) attack on the country's email and banking systems. The attackers bombarded Estonia's computer systems with one thousand times their normal rate of incoming email traffic. The campaign appeared to be well financed, suggesting backing by the Russian government. After three weeks, Estonian security officials, with help from outside experts, were able to stop the attacks by bolstering their server capacity and identifying and blocking incoming traffic from each of the hijacked machines.

The Estonian attacks were known as Cyber War I because they were the first instance of a sustained, large-scale, and politically motivated cyber assault on a country's digital infrastructure. Overall, however, the damage was minimal. The Estonian parliament's email system was inoperable for four days, customers of the country's two largest banks were unable to access their accounts for a few hours, and the country's largest daily newspaper had to temporarily disable overseas access to their sites. Some experts believed that the attackers were not trying to inflict serious damage with the attack, but instead were using it to attract attention to their political protest (Ruus, 2008).

2.2.2 Russia and Georgia, 2008

In August 2008, tensions boiled over between the country of Georgia and the Russian Federation over South Ossetia, an autonomous region on the Russia-Georgia border. South Ossetia had officially become independent in 1991, but Georgia and the international community still considered it part of Georgia. On August 7, the Georgian military launched a surprise assault on separatist forces in South Ossetia. Russia responded the next day with a military invasion into Georgia.

The military invasion was preceded by a cyber-assault on Georgia's web infrastructure. This consisted of defacements to government websites and a DDoS attack on numerous servers, similar to the Estonian attack. The websites of the president of Georgia and the Georgian Ministry of Foreign Affairs were defaced by a collection of photos of Mikheil Saakashvili and Adolf Hitler. Various government, banking, and news websites were also hit with DDoS attacks lasting up to six hours, with data rates up to 814.33 Mbps (Arbor Networks, 2008).

Russian websites were also covered with instructions on how to attack Georgian servers and distributed a script that was designed to attack Georgian sites. This suggested to some observers that the attacks were at least tolerated, if not directly supported, by the Russian Federation.

For the early days of the conflict, communication was shut down between the Georgian government and people, and between Georgia and the outside world, by the attacks. Although there were no long-lasting effects of the attack, for a few days it left the Georgian government unable to communicate with its own people or to spread its message about the conflict with Russia to the rest of the world. Banking services in the country were also temporarily shut down. The Georgian incident was notable as it was the first military conflict that was accompanied by a public, large-scale cyber assault (Tikk, E., Kaska, K., Runnimeri, K., Kert, M., Taliharm, A.-M., and Vihul, L., 2008).

2.3 Attacks on the U.S.

Here at home, cyber-attacks on U.S. networks and servers continued throughout the early 2000s. Two notable incidents are the power grid probes in 2009 and Operation Aurora.

2.3.1 Power Grid Intrusions

In April 2009, the U.S. government reported that cyber attackers had repeatedly breached the American power grid. The attacks were believed to have originated in Russia and China, despite denials by both countries. These attacks did not result in any damage; U.S. officials believed they were made to gather information about the power grid and map out the network. Officials also believed the attackers installed software that could be used at a later time to degrade the system. The penetration attempts were successful even though Congress had

allocated over $17 billion in the previous eight years to update the U.S. critical infrastructure to prevent cyber-attacks (Gorman, 2009).

2.3.2 The first large-scale corporate attack: Operation Aurora

In January 2010, the search engine company Google announced it had been the target of a "highly sophisticated" attack that originated in China on its corporate network. The attackers had used a dozen pieces of malware and several levels of encryption to carry out and conceal the attack, which resulted in the theft of intellectual property. McAfee later announced the Google attack was part of a coordinated assault, called Operation Aurora, on at least 34 companies. The attacks were apparently aimed at the companies' source code repositories. The intrusions ended when the U.S. servers that were used to coordinate them were shut down, though experts were unable to determine whether the attackers themselves or another party shut down the servers.

Operation Aurora was the largest coordinated cyber-attack on the U.S. commercial industry. "We have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack," said Dmitri Alperovitch, vice president of threat research for McAfee at the time. "It's totally changing the threat model" (Zetter, 2010).

3. The U.S. responds to the threat

Throughout the early 2000s, the cyber-attacks continued to increase in frequency and sophistication. Between 2006 and 2012, online attacks just on federal government information systems increased by 782%. In 2012, there were 48,000 reported incidents (U.S. Government Accountability Office, 2013).

By 2012, leaders in the federal law enforcement and defense communities were publicly issuing dire warnings about the threat of online attacks. In a hearing before the Senate Select Intelligence Committee, FBI Director Robert Mueller said, "stopping terrorists is the number one priority for the United States, but down the road, the cyber threat will be the number one threat to the country" (Mueller, 2012).

Defense Secretary Leon Panetta pointed to increasing technological capability and aggressiveness by adversary nations and said, "An aggressor nation or extremist group could use these kinds of cyber tools to … contaminate the water supply in major cities, or shut down the power grid across large parts of the country" (Bumiller, 2012). The most worrisome scenario,

which Panetta called a cyber-Pearl Harbor, involves "cyber-actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack" (Bumiller, 2012).

3.1 DoD builds up its cyber arsenal

Throughout the early 2000s, the federal government began building its cyber defenses, led by the DoD. In 2009, the secretary of defense directed the commander of U.S. Strategic Command to create U.S. Cyber Command (USCYBERCOM), which was tasked as the centralized agency for managing and improving DoD's cyber capabilities and conducting cyber operations (U.S. Cyber Command, 2010). USCYBERCOM includes 6,000 military and civilian personnel from all four military services who are trained in basic IT and specialized cyber security skills. Each service also maintains its own cadre of information security people.

The DoD is expanding its cyber security force even more to prepare for future threats. The Navy, Air Force, and Marine Corps each plan to add 1,000 people to their cyber workforces by 2016. The Army's cyber command is planning the construction of a 1,500-person cyber security command center (McCaney, 2013). The Pentagon also plans to add 900 people to USCYBERCOM's staff by 2016, with 80 percent of those slots for military personnel and 20 percent for civilians (Tilghman, 2013).

3.2 The U.S. goes on the offensive

There are also reports the U.S. is building its cyber-attack capabilities and has already used such capabilities in the past. During the 1999 bombing campaign against Serbia and Kosovo, the DoD reportedly formed an information operations cell to conduct information operations against Serbian targets. The cell, "which was composed of military personnel with expertise in various facets of IO," had "great success" during the war. The Air Force Office of Information confirmed that cyber warfare had a major role in the campaign, and an outside military expert asserted that the cell likely executed attacks against the Serbian air defense system. The results convinced DoD officials that cyber warfare has "an incredible potential," and "properly executed, could have halved the length of the campaign" (Brewin, 1999).

In 2011, Deputy Secretary of Defense William Lynn said that while DoD was opposed to militarizing cyber space, its strategy for preventing cyber-attacks included a deterrent approach based on the threat of retaliation.

Likewise Gen. James Cartwright, vice chairman of the Joint Chiefs of Staff, said the Pentagon had to shift from a mainly defensive posture to include a credible offensive capability. "If it's OK to attack me and I'm not going to do anything other than improve my defenses every time you attack me, it's very difficult to come up with a deterrent strategy," he stated. Cartwright pointed out most viruses are only a couple hundred lines of computer code, but the patches to fix the holes they exploit can run into millions of lines of code. So, "every time somebody spends a couple hundred dollars to build a virus, we've got to spend millions. So we're on the wrong side of that. We've got to change that around." (Alexander, 2011)

During his confirmation hearings to become the director of USCYBERCOM, Lt. Gen. Keith Alexander described the command's mission to include offensive cyber operations, carried out against military targets such as command and control systems, air defense networks, and weapons systems, but also potentially against civilian institutions that are essential to state sovereignty and stability, including power grids, financial, transportation, and telecommunications networks (Shanker, 2010).

Military leaders have reported that cyber warfare was being used in conjunction with operations in the Middle East. Marine Corps Lt. Gen. Richard Mills said at a military conference, "I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact." (Gjelten, 2013).

In 2010, the Stuxnet computer worm, a 500 kilobyte, highly sophisticated and malicious piece of code, attacked at least 14 industrial sites in Iran (Kushner, 2013). The malware, reportedly developed jointly by the U.S. and Israel, allowed its authors to spy on the industrial sites and, according to government reports, caused centrifuges vital to Iran's nuclear program to tear apart, setting the program back by up to two years.

A report by the New York Times indicated Stuxnet was part of a series of cyber-attacks on Iran's nuclear enrichment program, begun by the Bush Administration and accelerated when Obama took office. The last of the attacks temporarily took out nearly 1,000 of Iran's 5,000 centrifuges (Sanger, 2012).

The worm, which was ten times as large as a typical computer worm, induced rapid changes in the rotation speed of centrifuge motors, which would eventually cause them to blow apart. In order to keep the Iranians from knowing what was happening, Stuxnet secretly recorded normal readings at the plants and played those back, so that technicians would think everything

was working properly. Soon the Iranian engineers were going out to the centrifuges with two-way radios, trying futilely to reconcile what the instruments were saying with what they were seeing with their eyes. The idea, according to one source, was to make the Iranians "feel stupid" (Deibert, 2013, p.179).

Recent news reports indicate that U.S. military commanders are continuing to amass large numbers of people and resources to prepare for offensive cyber-attacks, and that those cyber-attacks are being used independently of traditional wartime operations.

Said Jason Healey, a former Air Force officer and director of the Cyber Statecraft Initiative at the Atlantic Council, "It might happen that we will use them as an adjunct to kinetic, but it's quite clear that we're using [cyber] quite a bit more freely" (Gjelten, 2013).

Some reports have gone much further. Respected information security expert Bruce Schneier asserts:

> "Today, the United States is conducting offensive cyberwar actions around the world. More than passively eavesdropping, we're penetrating and damaging foreign networks for both espionage and to ready them for attack. We're creating custom-designed Internet weapons, pretargeted and ready to be 'fired' against some piece of another country's electronic infrastructure on a moment's notice" (Schneier, 2013).

Schneier points to Presidential Policy Directive 20, issued on October 2012 and released by former National Security Agency contractor Edward Snowden, which spelled out US cyber war policy. He highlights two paragraphs in the directive that had been marked Top Secret, and that described Offensive Cyber Effect Operations (OCEO):

> "OECO can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging. The development and sustainment of OCEO capabilities, however, may require considerable time and effort if access and tools for a specific target do not already exist."
>
> "The United States Government shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated

as appropriate with other US offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive" (Schneier, 2013).

According to Snowden, the NSA has a cyber-warfare system under development called MonsterMind that could automatically block a cyber-attack against the U.S. and then launch a retaliatory counterattack, all without human intervention (Gross, 2014).

Although some may consider such a system beyond the capabilities of current technology, Schneier says the NSA and USCYBERCOM are already laying the groundwork by penetrating foreign computer networks and gathering information about them, in order to custom-design cyber weapons that will be effective against each of those networks.

4. 2012-2014: Cyber Attacks Proliferate

In the last two years, the number of cyber-attacks, and the number of countries launching such attacks, has multiplied. A report by Verizon found that data breaches in 2012-2013 originated in 40 different countries (Sofia Globe, 2013). Romania was second behind China in number of attacks against other countries, and Bulgaria, Russia, and the U.S. were also high on the list. While China and Russia are well known for conducting cyber intrusions against Western countries, other nations have become increasing threats. Particularly, countries that were targets of previous U.S. cyber-attacks have recently launched campaigns of their own.

In 2012, Iran was implicated in a series of attacks on the websites of U.S. banks Chase and Bank of America, and DDoS attacks against telecommunications companies AT&T and Level 3 (Nakashima, 2012). Earlier this year, news reports indicated that Iranian attackers were able to penetrate the Navy Marine Corps Internet for several months, although no data was believed to have been taken (Foxnews, 2014).

Some security experts believe the attacks are in retaliation for the earlier U.S. attacks against Iranian nuclear centrifuges. According to Gregory Rattray, chief executive officer of cyber security company Delta Risk, "If you are in the glass house, you should not be the one initiating throwing rocks at each other. We will have rocks come back at us" (Nakashima, 2012).

The Iranian attacks so far have caused only minor delays and disruptions, but they demonstrate the capabilities and determination of the Iranian government. "The Iranians aren't

very good yet," said one U.S. intelligence official, "But they're getting better rapidly, and they're motivated to get better rapidly because they believe they've been attacked, and they have" (Nakashima, 2012).

Iran's ally Syria has also been ramping up its cyber warfare capabilities. In 2013, a group of cyber attackers called the Syrian Electronic Army brought The New York Times website offline for over 20 hours. The attackers also penetrated the Twitter account of the Associated Press and issued a fake news alert, causing a brief panic and U.S. stock markets to plunge temporarily (Todd and Brown, 2013).

Across the world, meanwhile, North Korea is known to be intent on developing its cyber offensive capabilities (Osborne, 2014). The government is estimated to have around 3,000 to 6,000 trained cyber warriors, and South Korea claims that North Korea's cyber warfare group ranks behind only the U.S. and Russia as the world's largest cyber unit. Although North Korea often sponsors attacks through China and other nations, attacks in 2004 on U.S. State Department and DoD computers were attributed to the country.

5. Legal implications

Cyber warfare has emerged as a global threat so quickly that U.S. and international laws have not kept up. Legislation that is applicable to digital communication, such as the Electronic Communications Privacy Act and Digital Millennium Copyright Act, have been directed mainly at protecting the privacy and rights of individuals and corporate entities. Although there have been various executive policies issued, the laws governing cyber security are still being enacted.

Certainly, cyber defense raises some privacy and individual rights questions. If a company discovers its network is being used to plan a cyber-attack against another company's or the government's systems, does it have the right and obligation to notify the intended target and share the details of its findings? If the government has credible information that an attack is imminent, does it have the right to monitor all incoming email traffic to help determine the source of the attack?

A 2013 survey found that 62% of Americans think it is more important for the government to investigate possible national threats, even if that violates personal privacy. The public is evenly divided on whether monitoring email and other online communication is

acceptable to prevent possible attacks. Those views are mostly unchanged since shortly after the September 11 terrorist attacks (Pew Research Center, 2013).

The 2003 National Strategy to Secure Cyberspace (White House, 2003) and Homeland Security Presidential Directive 7 (U.S. Department of Homeland Security, 2012) designate the Department of Homeland Security (DHS) as the lead for coordinating the protection of the nation's electronic infrastructure.

One initiative deployed by the DHS in 2004 is the Einstein program, which is intended to detect cyber-attacks against federal agencies. Under the Einstein program, data collection systems are placed at participating agencies' Internet access points to monitor data flow and compare it to a baseline. The data collected includes IP addresses and ports, timestamps and durations, packet lengths, and protocols (U.S. Department of Homeland Security, 2004). Einstein 3, deployed in 2013, is intended to actively prevent network attacks by reading Internet traffic on private networks in addition to government systems, and blocking potentially dangerous Internet traffic before it reaches a government system (Corrin, 2013).

Besides serious technical and budgetary problems, the Einstein program has also raised a host of privacy concerns, despite favorable legal reviews by the U.S. Department of Justice (2009a, 2009b).

Some of the concern is because of the secrecy surrounding the government's cyber security initiatives. Although the Bush Administration and DHS released limited information about the cyber security measures they were taking, including Einstein 3, most of the details of the initiatives remain classified, and there is continuing Congressional and public concern about overreaching. Another source of concern is the lack of a statutory framework for cyber-monitoring and active defense. Without explicit legal restrictions, what are the constraints on the executive branch in carrying out its cyber protection responsibilities?

Both of these concerns could probably be eased by the government acting in a transparent manner and consistently following legal restraints. First, Congress should enact legislation that authorizes and defines the actions and responsibilities of the executive branch in the area of cyber security. Despite multiple attempts, such legislation has been slow in coming, however.

In 2012, and again in 2013, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA), which would allow private companies to share consumers' personal data with other companies and the government even if there was a contract in place

prohibiting such sharing. The bill was defeated in the Senate in 2012, and in 2013 it was not taken up by the Senate, which is drafting its own version of the law. CISPA in its present form is opposed by civil liberties groups and President Obama has vowed to veto it without further privacy protections (Stern, 2013).

The basis for Americans' basic expectation of privacy is rooted in the Fourth Amendment to the U.S. Constitution, under which persons have a right to be secure in their personal property against "unreasonable searches and seizures" (Amendment IV to the United States Constitution, 1789). Later court cases have determined that the restriction against an unreasonable search and seizure only applies when the person has a reasonable expectation of privacy (Lotrionte, 2012). In particular, the U.S. Supreme Court has ruled that, while contents of emails are protected, IP addresses and email addresses are not (United States v. Forrester, 2008). The privacy expectation has also been interpreted to apply only if another human would eventually see the private information if it were divulged (Lotrionte, 2012).

Therefore, automated monitoring of network traffic, conducted entirely by machines without human examination of the data collected, will not violate the terms of the amendment. The exception is more complete if the monitoring is general in nature (not directed at any specific person) and not used for law enforcement purposes; that is, the monitoring and analysis is only used for protecting government networks as a whole and not to look for evidence of criminal wrongdoing. Such monitoring is similar to the searching of passengers' property in subway stations and airports, the legality of which has been upheld (United States v. Edwards, 1974). Therefore, an explicit legal framework based on the Fourth Amendment and similar previous court cases would go far in setting the authorization and defining the scope of the government's cyber security policies.

Regular reviews could also help alleviate concerns about privacy and overreaching. The cyber security programs could be subject to regular Congressional reviews and also be required to publish regular reports, in unclassified form, about the status and recent actions under the programs. The programs could also undergo periodic legal review by independent experts with appropriate clearances to ensure that constitutional and statutory constraints are being followed. If significant discrepancies are found, the reviewers would have the authority to temporarily stop the discrepant aspects or at least convene meetings with the officials overseeing the programs.

Offensive cyber operations pose another set of issues. Present international law is unclear about what is permissible in cyber warfare, and even what constitutes a cyber-attack. Additionally, there are multiple international organizations that might have jurisdiction, such as NATO, the United Nations, and the Organization of American States (Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., and Spiegel, J., 2011). Furthermore, resolutions by such international governing bodies are often unenforceable. A system of treaties, similar to those governing nuclear and chemical weapons and military use of space, is needed to define and govern nations' activities in cyberspace.

5.1 Cyber security in the commercial sector

Commercial companies have a crucial role in protecting the nation's electronic infrastructure. Corporations produce most of the hardware and software used in this country, including IT security tools. Much of the Internet traffic runs on corporate networks. Government contractors carry out vital defense functions, collect, and process much of the intelligence data needed by national intelligence agencies. Additionally, corporations process financial transactions needed to fund defense and intelligence operations.

Despite this crucial role, there are regular news reports of significant IT security breaches at major corporations. Many of these incidents cost the companies involved millions of dollars or more in lost revenue and business. Some believe these are indications that corporations might not attach an appropriate sense of importance to cyber security (Etzioni, 2013).

Part of the reason may be cost. Information technology systems and services are expensive to an organization. The Gartner Group estimated in 2008 that global spending on IT equipment, software, and services, including telecommunications, was $3.4 trillion. Information security expenditures made up about 5% of the total, or $170 billion (Tully, Hale, Hahn, Hardcastle, Correia, and Brant, 2008).

To paraphrase a well-known saying, 'If you think education is expensive, try ignorance', one might equally well say, 'If you think security is expensive, try a break-in'. In late 2013, the retailer Target revealed that cyber thieves had penetrated its corporate networks and stolen up to 70 million customers' personal information such as their name, address, phone number and e-mail address. Up to 40 million may also have had their credit or debit information stolen (Isidore, 2014). The company suffered not only negative publicity and decreased revenue during the 2013

holiday shopping season (Bloomberg, 2014), but now faces some 140 lawsuits by banks and individuals, which some legal experts think may end up costing the company billions (Laver, Luongo, & Kendric, 2014).

The cost is not only to the corporations themselves. Data thefts at major defense contractors by attackers believed to be in China have resulted in the loss of plans for the F-35 Stealth Fighter (Freedberg, 2013). A report by the Senate Armed Services Committee indicated there were over 50 successful cyber intrusions or other incidents against U.S. Transportation Command contractors in 2012 and 2013. The report stated that the vast majority of information related to DoD deployments and distribution during both peacetime and wartime is transmitted over unclassified private networks similar to those that had been penetrated. The report went on to state that Chinese military doctrine specifically advocates attacking an adversary's command and control and logistics networks to degrade their ability to operate in the early stages of a conflict (Senate Armed Services Committee, 2014).

Another problem may be that companies currently have little incentive to follow sound IT security practices. A commonly cited example is credit cards. Starting in the 1970s, the government placed strict limits on customers' responsibility for fraudulent charges; this change led credit card companies to begin implementing necessary security measures (Etzioni, 2013).

Companies' primary reason for being in business is to make a profit, not necessarily to look out for the national interest. Protecting the nation's infrastructure is the role of the government. Unlike corporations, the government can and does spend large amounts of money on programs intended to further the national interest without requiring any monetary return.

There is a role for the government in private sector-based IT security. According to a 2014 survey by Dell, 90 percent of IT companies worldwide would like government to be involved in helping the private sector create a solid security strategy and protect organizations against internal and external threats (Malykhina, 2014).

The government also has a strong incentive to promote security in private companies. As previously mentioned, corporations run many critical functions on behalf of defense and intelligence agencies and create most of the hardware and software that these agencies use. But both the government and private sector have opposed government dictating specific security measures for private companies, and rightfully so.

5.2 Government-Private security partnerships

Instead of a specific set of policies, the government might create a set of voluntary security guidelines for companies and set financial incentives to follow them. Many times, companies fail to spend adequately on IT security practices because it is hard to measure the return on investment. A system of incentives would help with such measurements.

Companies that had security incidents and were found to be lacking in security measures would have financial penalties imposed. The proceeds would be used for financial restitution for parties injured by the incident. Customers who had their personal data compromised might receive several years of free enrollment in identity theft protection services; other companies that had loss of revenue because of the incident would be compensated.

The incentives would be commensurate with the amount and sensitivity of data handled by the organization, so that large corporations that process terabytes of critical defense data or individuals' personal information would have a larger incentive than smaller companies that store megabytes of data or less critical information.

The IT security guidelines issued by the government would be basic, common sense security measures that security providers' advocate, but organizations too often fail to follow. These include technical security measures like intrusion detection and prevention systems, antivirus software, and regular patching and updates. They would also include administrative measures like strong, regularly changed passwords, separation of duties, least privilege, prompt deletion of accounts of employees who have left the organization, and proper incident response and handling procedures.

The Twenty Critical Security Controls represents a reasonable basis for identifying security measures that should be implemented in private companies. The controls were originally developed at the request of the DoD to help prioritize its cyber security efforts and focus on the security controls that were most effective in stopping known attacks since the early 2000s (SANS, n.d.(a)). After extensive discussions by a large consortium of government agencies in the U.S. and United Kingdom and major U.S. private security companies, the list of twenty controls was published in 2008. The controls have since been revised and are currently in Version 5 (SANS, n.d.(b)).

After independent analysis, the U.K. government announced in 2011 that it would adopt the Twenty Critical Controls as the framework for securing its critical infrastructure. The commander of USCYBERCOM, Army Gen. Keith Alexander, endorsed the controls in 2012. Testing by the U.S. Department of State and Department of Energy found the controls matched very well with actual threats and previous cyber-attacks.

Furthermore, surveys of system and security administrators found that 80 percent of respondents believed that adopting the controls would lower their security risk, and 80 percent of those who had implemented the controls believed that they had already reduced risk.

The controls include both technical and administrative types of measures. The majority of organizations have installed technical security tools, but often fail to install or use them properly and follow safe personnel processes. Simple measures like regularly changing passwords and restricting administrative privileges will go a long way toward reducing security risk (Dittmer, 2014).

One very useful security measure is creating and enforcing an information security awareness program among all employees (Dittmer, 2014). The program should include policies and guidelines, periodic security awareness training, and incentives for compliance. In a large organization with a diverse staff, senior management can convene a working group to help create and review the policies and training materials to ensure various language and cultural norms are respected.

Besides basic employee security training, those in crucial security roles, such as system and security administrators, should be properly trained to fulfill those roles. Too often, tasks like information assurance are assigned to individuals who have not received the required training. Technical personnel should receive initial and ongoing training in the critical controls that apply to their duties.

All training programs and policies should be presented to senior management for review and approval. A single senior executive is typically assigned to oversee this project. Senior management approval provides needed organizational support to the policies and programs and also commits the needed resources to implement them.

Social media is another major security issue: many employees connect their personal mobile devices to the company network and download apps without thought to the security of the software or the organization. The organization's policies must address this as well. Again, the

extent of the security measures expected of an organization would depend on the organization's size and the criticality of the information processed. Employment of skilled security staff and tools to implement these measures may not be cheap, but would help the organization avoid greater potential costs in the future. The requirements would apply across the board, so no company could claim to be at a disadvantage relative to its direct competitors.

Software developers that create software used for defense, intelligence, or other vital government functions should be required to follow secure software development processes, with security and reviews built in to the entire software development life cycle. Secure development practices are now a focus of attention in the IT community. According to InfoWorld, the Certified Secure Software Lifecycle Professional (CSSLP) certification, sponsored by the International Information Systems Security Certification Consortium ((ISC)²), is second place among 2014's highest paying IT certifications (Hein, 2014).

Companies that refuse to comply would risk losing federal business. Before the 1990s, the DoD used expensive but secure custom-made software; in the late 1990s, Microsoft successfully convinced DoD officials to use its operating systems. Despite well-publicized failures like the USS Yorktown smart ship in 1998 (Wired, 1998), the DoD continues to use Windows and other commercial off-the-shelf software. Many are urging a switch to Linux and other open-source software, which can be inspected for flaws and customized for specific requirements (Etzioni, 2013).

Early on, Microsoft steadfastly refused to share its source code with the government or other entities and lobbied intensely in opposition to information sharing. Starting in the early 2000s, Microsoft changed its policy and began making agreements to share the source code of its operating systems with the U.S. and other governments in order to increase confidence in the systems' security (Microsoft, 2003). Microsoft also shares its code with private sector partners. This is definitely a move in the right direction for all parties concerned.

The government has made some tentative moves toward addressing security deficiencies in the private sector. Under a plan proposed by the Obama Administration, private companies would be required to report security breaches to the affected individuals and the Federal Trade Commission (FTC) within 60 days. The FTC would be responsible for imposing penalties for failure to make such reports. This measure is intended to incentivize organizations to identify and fix security lapses (Etzioni, 2013).

Effectively countering national cyber threats requires information sharing between the government and private sector, and this has traditionally been an obstacle. Present policies and laws on both sides tend to discourage information sharing. Government agencies are often reluctant to share their information about cyber threats with industry because of the sensitive nature of the intelligence, and corporate executives are hesitant to share with the government because of concerns about exposure of confidential information. Meanwhile, antitrust laws discourage cooperation among companies.

Steps have been taken, however, to address this obstacle. Current guidelines set by the Department of Justice and FTC in fact do not prohibit information sharing as long as it does not negatively affect competition. Earlier this year the two agencies publicly clarified their position by emphasizing that sharing of cyber security information including incident or threat reports, threat signatures, and alerts is not an antitrust violation (Jackson, 2014). Additionally, under a proposed plan from the Obama Administration, companies would be immune from liability if they voluntarily shared threat information with the Department of Homeland Security for cyber-investigations (Etzioni, 2013).

There have also been steps taken to promote sharing on the government side. In a 2013 executive order, the Obama Administration underscored the need for the government to share cyber threat information with the private sector. In 2013, the federal government notified over 3,000 companies that their information systems had been attacked, a number believed to account for only a fraction of actual attacks (Nakashima, 2014). Nevertheless, it represented a milestone in increased sharing of threat information between the government and private companies.

The DoD Defense Industrial Base (DIB) Cyber Security/Information Assurance (IA/CS) Program is an example of a government-private collaboration to improve private sector security. It is "a voluntary program to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits, DIB unclassified information systems" (Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS\IA) Program, n.d.).

Under the program, participating companies receive tools and assistance to help protect critical defense data and to limit the damage if a security incident occurs. The DoD shares information about cyber security threat indicators with the companies. Each company is free to incorporate this information into its security monitoring tools and take other actions as it sees fit.

The DoD also shares techniques to mitigate the effects of a cyber-security incident (Department of Defense, 2012).

6. Is cyber warfare "real"?

One might be inclined to ask, is cyber warfare a tangible threat? Defacement of websites can be embarrassing, temporary loss of use of communication and banking sites can cause inconvenience, and theft of intellectual property can hurt a company's revenues. But, can malevolent bytes flowing across cyberspace actually cause bodily harm? Could cyber terrorists or hostile foreign cyber warriors kill Americans with a keyboard?

Certainly some analysts have made the case that cyber warfare may be a more humane type of warfare because there are far fewer casualties. This has been true of cyber conflicts so far, but will continue to remain so only under certain conditions. These conditions include vital facilities sufficiently protecting themselves to be impervious to the effects of a cyber-attack, and countries refraining from responding to a cyber-attack with conventional military action (Maurer, 2011).

At present, however, these conditions do not exist. Critical infrastructures of the U.S. and other nations remain vulnerable to serious disruption from cyber-attacks, and cyber-attacks are very often used in conjunction with conventional military campaigns. There are at least four reasons why cyber-attacks should be considered a legitimate threat.

First, cyber warfare is often used to accompany, not replace, conventional warfare. The U.S. cyber operations in Serbia in 1999, and the attacks on Estonia in 2007 and Georgia in 2008 illustrate this. These cyber-attacks significantly enhanced the effectiveness of these conventional military operations.

Second, theft of sensitive information can lead to more than loss of a company's revenue. Theft of customers' personal information can aid criminals in carrying out fraud and identity theft. Likewise, theft of sensitive information from government servers can compromise the nation's military and intelligence positions and significantly degrade the nation's technological capabilities, while increasing those of an adversary.

Third, cyber warfare can have physical effects. According to Bruce Schneier, "Cyberattacks have the potential to be both immediate and devastating. They can disrupt communications systems, disable national infrastructure, or, as in the case of Stuxnet, destroy

nuclear reactors" (Schneier, 2013). In 2000, a disgruntled former employee of a sewage equipment installation company in Australia used radio equipment and a computer to cause 800,000 liters of raw sewage to flood into rivers, local parks, and even onto the grounds of a Hyatt Regency hotel. According to reports, "Marine life died, the creek water turned black and the stench was unbearable for residents" (Abrams & Weiss, 2008). This was the first widely publicized instance of someone maliciously penetrating a utility control system.

Finally, most industrialized nations in the world are heavily dependent on technology. The societies in the United States and many other countries literally could not function if their digital networks were to break down significantly for an extended length of time. A country that experiences a major disruption to its electronic infrastructure at the hands of another country, whether accidental or intentional, very well might view such an incident as an act of war and respond with a conventional military strike.

7. Conclusion

Although significant advances have been made in the U.S. cyber security posture in the last decade, especially in the federal government, major deficiencies remain. Recent unfortunate events in Iraq and Syria amply demonstrate that there is no shortage of individuals in the world who desire to inflict severe harm on America and Americans. That a major cyber-attack has not occurred thus far on the U.S. might be attributed more to a lack of means and opportunity than of motivation. Incidents like the power grid probes of 2009 show that our infrastructure is vulnerable to a determined, trained, and well-funded adversary. In the future, more of our electrical grids will likely be connected to the same network, and our homes, cars, household appliances, and even medical devices will likely be connected to the Internet. This will greatly increase the potential for security issues.

This paper has presented some suggestions for addressing cyber security deficiencies in the administrative and policy areas and resolving the legal issues associated with cyber security policy. It is incumbent upon both the government and private sector to put in place the security controls and legal frameworks needed to resolve major remaining cyber security shortcomings and prepare adequately for future cyber-attacks.

8. References

Abrams, Marshall & Weiss, Joe. (2008, July 23). Malicious control system cyber security attack case study: Maroochy Water Services, Australia. Retrieved August 11, 2014, from http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

Alexander, David. (2011, July 14). Pentagon to treat cyberspace as "operational domain". Retrieved August 16, 2014, from http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714

Amendment IV to the United States Constitution (1789). Retrieved August 20, 2014, from http://www.law.cornell.edu/constitution/fourth_amendment

Andress, J. & Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham, MA: Syngress.

Arbor Networks (2008, August 12). Georgia DDoS attacks – a quick summary of observations. Retrieved August 29, 2014, from http://www.arbornetworks.com/asert/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

Bloomberg (2014, January 13). Target reports direct financial impact from customer payment card breach. Retrieved August 10, 2014, from http://www.bna.com/target-reports-direct-n17179881326/

Brewin, Bob. (1999, September 27). Kosovo ushered in cyberwar. Retrieved August 17, 2014, from http://fcw.com/Articles/1999/09/27/Kosovo-ushered-in-cyberwar.aspx

Bumiller, E. (2012, October 11). Panetta Warns of Dire Threat of Cyberattack on U.S. Retrieved August 7, 2014, from http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0

Corrin, Amber. (2013, July 26). DHS rolls out Einstein intrusion detection. Retrieved August 19, 2014, from http://fcw.com/articles/2013/07/26/einstein-rollout.aspx

Daly, John. (2006, October 9). US Air Force Prepares For Cyber Warfare. Retrieved August 11, 2014, from http://www.spacedaily.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html

Defense Industrial Base (DIB) Cyber Security / Information Assurance (CS\IA) Program, (n.d.). Retrieved September 2, 2014, from http://dibnet.dod.mil/

Deibert, Ronald J. (2013). *Black Code: Inside the Battle for Cyberspace.* Toronto: McClelland & Stewart.

Department of Defense (2012, May 11). Fact sheet: Defense Industrial Base (DIB) cybersecurity activities. Retrieved September 2, 2014, from http://www.defense.gov/news/d20120511dib.pdf

Dittmer, John (2014, August 7). *Implementing an information assurance awareness program: A case study for the Twenty Critical Security Controls at Consulting Firm X for IT personnel.* Retrieved August 30, 2014, from http://www.sans.org/reading-room/whitepapers/bestprac/implementing-information-assurance-awareness-program-case-study-twenty-critical-secur-35322

Drogin, B. (1999, October 7). Russians seem to be hacking into pentagon / sensitive information taken -- but nothing top secret. Retrieved August 3, 2014, from http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php

Etzioni, A. (2013, November 27). Cybersecurity in the private sector. Retrieved August 10, 2014, from http://issues.org/28-1/etzioni-2/

Foxnews (2014, February 18). Iranian hacking of Navy computers reportedly more extensive than first thought. Retrieved October 22, 2014, from http://www.foxnews.com/politics/2014/02/18/iranian-hacking-navy-computers-reportedly-more-extensive-than-first-thought/

Freedberg, Jr., Sydney J. (2013, June 20). Top official admits F-35 Stealth Fighter secrets stolen. Retrieved August 29, 2014, from http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/

Gjelten, Tom. (2013, January/February). First strike: US cyber warriors seize the offensive. Retrieved August 17, 2014, from http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive

Gorman, S. (2009, April 8). Electricity grid in U.S. penetrated by spies. Retrieved August 5, 2014, from http://online.wsj.com/news/articles/SB123914805204099085

Gross, Grant. (2014, August 13). Snowden reveals automated NSA cyberwarfare program. Retrieved August 20, 2014, from http://www.infoworld.com/d/security/snowden-reveals-automated-nsa-cyberwarfare-program-248297

Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., and Spiegel, J. (2011, November 16). The law of cyber-attack. Retrieved August 20, 2014, from www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf

Hein, R. (2014, August 15). *2014's* hottest IT certifications. Retrieved August 20, 2014, from http://www.infoworld.com/slideshow/161879/2014s-hottest-it-certifications-248455?source=IFWNLE_nlt_daily_am_2014-08-15

Hildreth, S.A. (2001, June 19). *Cyberwarfare.* CRS Report for Congress. Retrieved August 3, 2014, from http://fas.org/irp/crs/RL30735.pdf

Isidore, Chris. (2014, January 11). Target: Hacking hit up to 110 million customers. Retrieved August 10, 2014, from http://money.cnn.com/2014/01/10/news/companies/target-hacking/

Jackson, W. (2014, April 11). Feds address antitrust concerns on cyberthreat sharing. Retrieved August 16, 2014, from http://www.informationweek.com/government/cybersecurity/feds-address-antitrust-concerns-on-cyberthreat-sharing/d/d-id/1204403

Konkel, F. (2014, August 21). Amazon expands its cloud services to the U.S. military. Retrieved August 22, 2014 from http://www.defenseone.com/technology/2014/08/amazon-expands-its-cloud-services-us-military/92090/

Kushner, David. (2013, February 26). The real story of Stuxnet. Retrieved August 17, 2014, from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Laver, Seth, Luongo, Michael P., and Kendric, Christopher (2014, May 29). The Target data breach litigation begins. Retrieved August 10, 2014, from http://professionalliabilitymatters.com/2014/05/29/the-target-data-breach-litigation-begins/

Loney, M. (2004, March 1). US software 'blew up russian gas pipeline'. Retrieved August 2, 2014, from http://www.zdnet.com/us-software-blew-up-russian-gas-pipeline-3039147917/

Lotrionte, Catherine B. (2012). Cyber-search and cyber-seizure: Policy considerations of cyber operations and fourth amendment implications. In Reich, Pauline C. and Gelbstein,

Eduardo (Eds.), ***Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization.*** Hershey, PA: IGI Global.

Malykhina, E. (2014, February 26). Government cybersecurity guidance wanted by private sector. Retrieved August 6, 2014, from http://www.informationweek.com/government/cybersecurity/government-cybersecurity-guidance-wanted-by-private-sector/d/d-id/1113999

Maurer, Tim. (2011, October 19). The case for cyberwarfare: Why the electronic wars of the future will actually save lives. Retrieved August 12, 2014, from http://www.foreignpolicy.com/articles/2011/10/19/the_case_for_cyberwar

McCaney, Kevin. (2013, December 9). Army graduates its first class of cyber network defenders. Retrieved August 12, 2014, from http://defensesystems.com/articles/2013/12/09/army-cyber-network-defender-graduation.aspx

Menn, J. (2011, August 3). Cyberattacks penetrate military secrets and designs. Retrieved August 2, 2014, from http://www.ft.com/cms/s/0/d4f09016-bda3-11e0-babc-00144feabdc0.html

Microsoft Corporation (2003, January 14). A matter of national security: Microsoft government security program provides national governments with access to Windows source code. Retrieved August 29, 2014, from http://www.microsoft.com/en-us/news/features/2003/jan03/01-14gspmundie.aspx

Mueller, Robert S. III (2012, January 31). *Worldwide Threat Assessment of the US Intelligence Community.* Testimony at Senate Select Intelligence Committee hearing.

Nakashima, Ellen. (2012, September 21). Iran blamed for cyberattacks on U.S. banks and companies. Retrieved October 22, 2014, from http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

Nakashima, Ellen. (2014, March 24). U.S. notified 3,000 companies in 2013 about cyberattacks. Retrieved August 12, 2014, from http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html

Office of Legal Counsel. (2009a). Legal issues relating to the testing, use, and deployment of an intrusion-detection system (Einstein 2.0) to protect unclassified computer networks in the Executive Branch. Memorandum Opinion for the Counsel to the President. Retrieved

August 19, 2014, from http://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues.pdf

Office of Legal Counsel. (2009b). Legality of intrusion-detection system to protect unclassified computer networks in the Executive Branch. Memorandum Opinion for the Counsel to the President. Retrieved August 19, 2014, from http://www.justice.gov/sites/default/files/olc/opinions/2009/08/31/legality-of-e2.pdf

Osborne, Charlie. (2014, September 2). North Korea cyber warfare capabilities exposed. Retrieved October 22, 2014, from http://www.zdnet.com/north-korea-cyber-warfare-capabilities-exposed-7000033192/

Pew Research Center (2013, June 10). Majority views NSA phone tracking as acceptable anti-terror tactic. Retrieved August 20, 2014, from http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

Rashid, F. Y. (2013, June 25). Organizations Implementing, Seeing Benefits of Critical Security Controls: Survey | SecurityWeek.Com. Retrieved from http://www.securityweek.com/organizations-implementing-seeing-benefits-criticalsecurity-controls- survey.

Ruus, K. (2008). Cyber War I: Estonia attacked from Russia. Retrieved August 3, 2014, from http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html

Sanger, David E. (2012, June 1). Obama order sped up wave of cyberattacks against Iran. Retrieved August 17, 2014, from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

SANS (n.d.(a)) Critical Security Controls: A Brief History. Retrieved September 2, 2014, from http://www.sans.org/critical-security-controls/history

SANS (n.d.(b)) Critical Security Controls: Version 5. Retrieved September 2, 2014, from http://www.sans.org/critical-security-controls/controls

Schneier, Bruce. (2013, June). US offensive cyberwar policy. Retrieved August 19, 2014, from https://www.schneier.com/blog/archives/2013/06/us_offensive_cy.html

Shanker, Thom (2010, April 14). Cyberwar Nominee Sees Gaps in Law. Retrieved August 15, 2014, from http://www.nytimes.com/2010/04/15/world/15military.html?_r=1&

Sofia Globe (2013, April 24). Romania, Bulgaria among most frequent sources of cyber-attacks – report. Retrieved October 22, 2014, from http://sofiaglobe.com/2013/04/24/romania-bulgaria-among-most-frequent-sources-of-cyber-attacks-report/

Stern, Joanna. (2013, April 18). CISPA cybersecurity bill passes House, again. Retrieved August 20, 2014, from http://abcnews.go.com/Technology/controversial-cispa-cybersecurity-bill-passes-house/story?id=18992121

Taylor, P. (2011, August 10). Anatomy of a cyberattack. Retrieved August 2, 2014, from http://www.ft.com/cms/s/0/0ec77afc-c2cc-11e0-8cc7-00144feabdc0.html

Tikk, E., Kaska, K., Runnimeri, K., Kert, M., Taliharm, A.-M., and Vihul, L. (2008, November). Cyber attacks against Georgia: Legal lessons identified. Retrieved August 4, 2014, from http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

Tilghman, Andrew. (2013, February 12). Cyber Command to hire thousands of troops, civilians. Retrieved August 12, 2014, from http://www.defensenews.com/article/20130212/C4ISR01/302120026/Cyber-Command-Hire-Thousands-Troops-Civilians

Todd, Brian and Brown, Forrest. (2013, August 30). Syria's cyberattack: First wave of a bigger war? Retrieved October 22, 2014, from http://www.cnn.com/2013/08/30/tech/syria-cyberattacks/

Tully, J., Hale, K., Hahn, W. L., Hardcastle, J., Correia, J. M., and Brant, K. F. (2008). Dataquest insight: IT markets remain resilient in 2008 and will grow moderately in the next three to five years. Retrieved August 5, 2014, from http://www.gartner.com/DisplayDocument?ref=g_search&id=741014&subref=simplesearch

U.S. Cyber Command (2010, May 25). U.S Cyber Command Fact Sheet. Retrieved August 11, 2014, from http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf

U.S Department of Homeland Security (2004, September). Privacy impact assessment einstein program: Collecting, analyzing, and sharing computer security information across the federal civilian government. Retrieved August 19, 2014, from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf

U.S. Department of Homeland Security (2012, July 9). Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Retrieved August 19, 2014, from http://www.dhs.gov/homeland-security-presidential-directive-7

U.S. Government Accountability Office (2013, February). *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (GAO-13-187).

U.S. Senate Armed Services Committee (2014). *Inquiry into cyber intrusions affecting U.S. Transportation Command contractors*. Retrieved September 19, 2014, from http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf

United States v. Edwards, 498 F.2d 496 (1974, May 29). Retrieved August 20, 2014, from http://openjurist.org/498/f2d/496/united-states-v-edwards

United States v. Forrester, 512 F.3d 200 (9th Cir.) (2008). Retrieved August 20, 2014, from http://itlaw.wikia.com/wiki/U.S._v._Forrester

Vijayan, J. (2007, February 26). Q&A: Reverse hacker describes ordeal. Retrieved August 4, 2014, from http://www.computerworld.com/s/article/9011832/A_Reverse_hacker_describes_ordeal_?pageNumber=3

Wegilant (n.d.). What are Titan Rain attacks? Retrieved August 4, 2014, from http://www.wegilant.com/what-are-titan-rain-attacks/

White House (2003, February). National Strategy to Secure Cyberspace. Retrieved August 19, 2014, from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Wikipedia (2014, June 30). Shawn Carpenter. Retrieved August 4, 2014, from http://en.wikipedia.org/wiki/Shawn_Carpenter

Wired (1998, July 24). Sunk by Windows NT. Retrieved August 14, 2014, from http://archive.wired.com/science/discoveries/news/1998/07/13987

Zetter, K. (2010, January 14). Google hack attack was ultra sophisticated, new details show. Retrieved August 5, 2014, from http://www.wired.com/2010/01/operation-aurora

Last Updated: December 13th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	OnlineCAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced