PEPPERDINE UNIVERSITY

Pepperdine Policy Review

Volume 7 Article 3

6-17-2014

Much Ado about Cyber-space: Cyber-terrorism and the Reformation of the Cyber-security

Christian Pedersen
Pepperdine University, christian.pedersen.pepperdine@gmail.com

Much Ado about Cyber-space:

Cyber-terrorism and the Reformation of the Cyber-security

Christian Pedersen

Introduction

Acclaimed scholar and science-fiction writer Isaac Asimov stated, despite the destructive advances in technology, he did "not fear computers," instead he feared "the lack of them." In this day and age, security experts may have a very different opinion than Dr. Asimov. While computers have created many of the wonderful luxuries which make modern life possible; they create a whole series of new security threats. The magnitude of these security threats needs to be understood by policy makers and security experts alike.

In wake of revelations made by renegade NSA (National Security Administration) contractor Edward Snowden, politicians and the general public alike have called into question the intelligence and cyber efforts of the United States. Cyber-security is becoming national security. As President Obama and the US intelligence community wrestle with the monumental task of restructuring the NSA, they must adapt to the emerging threat that is cyber-terrorists and their ability to attack portions of critical United States infrastructure.

What is cyber-space? Why is it so important? What types of threats reside there? These are the questions a majority of the public, and many policymakers for that matter, must come to terms with. For centuries, there were two basic planes of existence in which all commerce, social interaction, political communication, and military operation occurred. This was the land and the

sea (Kramer, 2009, 25). This was life as humanity knew not only for centuries, but since the existence of mankind. However, at the beginning of the 20th century, the Wright brothers discovered manned flight. Within the matters of a few decades, two more realms of existence were conquered by humanity, air and space (Kramer, 2009, 25). Though each of these realms exists, each is very different. Each has different physical properties and characteristics, but there is no dispute that each of these realms exists. Early pioneers have explored them, human technology has allowed us to master them, and because of that technology human existence, to some degree, has occurred within each of them. In the last few decades, a fifth dimension of human existence has come into reality; this is cyber-space (Kramer, 2009, 25).

Unlike the other realms of existence, this realm was not simply discovered, it was created. Foundations for the modern internet were laid with the creation of the Advanced Research Projects Agency Network, or ARPANET, a computer network created by the U.S. Department of Defense (DOD) and four academic Universities (Clarke and Knake, 2010, 283). Although it was created by the human mind, its potential is still not fully understood. Cyber-space is rapidly evolving. Over the past few decades this realm has exploded with activity. Everything from commerce to education and innovation to social activism now exist within cyber-space in one form or another (Negroponte and Palmisano, 2013, 3).

The internet has grown at an overwhelming pace, which makes the creation of a lasting security policy and regulation difficult. Since inception the internet has rapidly consumed the planet. Currently, one third of the planet is connected online, and in a few short years it is estimated that another third of the planet will be online as well (Negroponte and Palmisano, 2013, 3). By the year 2020, approximately 40 years following the creation of the internet, nearly

5 billion people will have become participants in this new global community (Negroponte and Palmisano, 2013, 3).

A Target Ripe for Terrorism: Critical Digital Infrastructure

Aside from individuals connecting to the internet, businesses and government have connected as well, creating security hazards. Critical infrastructure computer systems are responsible for controlling or operating infrastructure components such as electricity, energy, water and sewer, as well as tele-communications (Shea, 2004, 2). This is also referred to as the digital infrastructure, since it is the digital counterpart to the physical infrastructure. These systems are connected to the internet and any system connected to the internet, can be hacked. This makes infrastructure systems major security risks. The number of systems integrated online is growing exponentially, as more and more systems become connected to the internet. This makes it harder and harder to identify potential targets (Crelinsten, 2009, 169). As the world becomes increasingly digitalized, the number of potential targets grows as well, making it increasing difficult to identify potential targets.

Two of the most important components of the digital infrastructure are supervisory control and data acquisition (SCADA) systems and distributed control systems. These systems represent the most critical components of cyber-security. SCADA systems, while they are not a source of information themselves, are responsible for controlling and monitoring operation systems (Shea, 2004, 5). In pipelines – such as water, oil, or liquid natural gas – SCADA systems are responsible for controlling values and monitoring flow (Shea, 2004, 5). Distributed control systems monitor and regulate systems of a single facility, such as a chemical production facility or a manufacturing plant (Shea, 2004, 5). In many instances, both of these types of systems work in conjunction, such as in power plants or in a water treatment facility. In a power plant,

distributed control systems monitor the plant, while SCADA systems monitor the entire power grid. Both of these systems are vulnerable to attack, but each attack would have different impacts. An attack on a distributed control systems will cripple a facility, while an attack on a SCADA system will damage the grid. Many of these control systems were originally separate from the internet, but were integrated to prevent redundancy and ensure uniformity (Shea, 2004, 6). While controlling these systems from a central location does improve efficiency, it also increases the security threat. Once systems become integrated into the internet their vulnerability to a cyber-attack increases dramatically.

The ramifications of this cannot be understated. In the past, someone wishing to cause mass destruction or wide spread chaos might plan an attack against a power plant. In order to sabotage that plant, they would need to overcome a series of physical barriers – fences, sentries, and locked doors. In the digital age, traditional security measures such as fences and secure facilities no longer matter (Sweetman, 2009, 31). Networks can be compromised and systems can be sabotaged by a hacker with a laptop, sitting anywhere in the world. So while the list of potential targets has exponentially grown, the number of potential terrorists has grown as well. In 2012 for example, the number of cyber-attacks on critical infrastructure systems grew by fifty-two percent (Goldman, 2013). Nearly half of theses attacks were directed towards energy systems, but attacks were also directed towards water systems, chemical facilities, and even nuclear facilities (Goldman, 2013).

Part of the problem in defending against cyber-attacks is that the infrastructure components most vulnerable to attack, are owned and operated by the private sector (Crelinsten, 2009, 169). While government defense and security systems may be targets of attack, the private sector owns more than eighty percent of the infrastructure most vulnerable to cyber-attacks

(Crelinsten, 2009, 169). Unfortunately, the cyber-security of some private systems has been somewhat of a low priority (Shea, 2004, 2). Some in the private sector believe that the lack of major cyber-attacks to date means that the threat is minimal (Shea, 2004, 9). This is the equivalent of saying that the threat of nuclear weapons is minimal, because so few have been used. Others in the private sector believe that a cyber-attack would have a minimal impact, as safe guards already exist in the event of natural disaster or system failure (Shea, 2004, 10).

During the Bush Administration, the private industry was largely left to self-regulate itself (Crelinsten, 2009, 169). While this may be in line with the spirit of Ronald Reagan, this is not necessarily in the best interest of homeland security. While some businesses have introduced the appropriate safe guards, others have failed to take the cyber-threats seriously and act responsibly (Crelinsten, 2009, 169). The failure of the United States government to successfully implement regulations, and the failure of private sector to successfully regulate their own networks, holds the United States at the mercy of the hackers. President Obama claims to have recognized the growing threat that of cyber-space, and has vowed to take these threats more seriously than his predecessors. In the most recent National Security Strategy distributed by the Obama Administration, the White House has committed the United States to adequately preparing to meet the threats residing in cyber-space, this include the emerging threat of cyber-terrorist attacks (White House, 2010, 17).

Traditional Terrorist Using Cyber-Space

The growing availability of computer technology has created new tools through which terrorist can plan and execute attacks. A cyber-terrorist attack is a disruptive digital attack on a computer system which creates fear or results in potential disorder (Rollins and Wilson, 2007, 17). These are cyber- attacks directed towards networks or computer systems by non-state actors,

either terrorist organizations or just individual hackers. The devastating potential of a cyber-terrorist attack on infrastructure systems led the former Secretary of Defense, Leon Panetta, to warn policymakers to prepare for the coming "cyber-Pearl Harbor" (Negroponte and Palmisano, 2013, 23). Those who agree with Panetta, remember the United States' failure to detect and prevent the terrorist attacks of September, 11, and fear the United States is doomed to repeat this same failure in the digital world (Lappin, 2011, 142).

A few known terrorist have shown interest in launching cyber-attacks (Clapper, 2013, 7). To date, there have been very few successful cyber-attacks executed as acts of terrorism; and the ones which have occurred have been minimal in scale and scope (Crelinsten, 2009, 169). Most of the attacks which have been connected to terrorists have been very basic, primarily attacking email accounts and websites (Rollins and Wilson, 2007, 4). Terrorist groups have been known to launch denial-of-service attacks, where they flood a website with phony hits in an attempt to overload and crash the server (Lappin, 2011, 106). They also have been known to hijack websites replacing them with messages, or sometimes they use threating videos or footage from previous attacks (Lappin, 2011, 108). The FBI believes that more sophisticated and complex cyber-attacks are on the horizon, as terrorist groups are showing an improved understanding of cyberspace (Rollins and Wilson, 2007, 4). Terrorist organization will be able to launch more damaging attacks, beyond simply attacking website, as they recruit or hire advanced hackers (Rollins and Wilson, 2007, 4). This will allow them to attack infrastructure systems and hack government servers (Rollins and Wilson, 2007, 4). Al Qaeda recruits are now trained in computer hacking in preparation for the "electronic jihad" (Rollins and Wilson, 2007, 17). It is known that some members are well trained in engineering and computer programming (Rollins and Wilson, 2007, 15). It is an established fact that al Qaeda has MIT educated scientist within

its ranks (Bergen, 2011, 215). As terrorist develop a better understanding of cyber-space, the belief in the intelligence community is that they will begin to launch attacks which cripple and disable infrastructure systems (Rollins and Wilson, 2007, 16).

There are many in the United States intelligence community who already believe that SCADA systems have already been identified as potential targets for terrorist attack. Nearly a decade ago in Afghanistan, laptop computers were found with detailed analysis of SCADA systems and vulnerabilities (Shea, 2004, 10). These included the SCADA systems controlling the electric grid and the water treatment facilities in San Francisco; it is quite clear that hackers in the Middle East intended to attacks these systems (Lappin, 2011, 143). This is not a completely foreign concept, as around the same time that the computer was found in Afghanistan, a hacker in Australia was apprehended attempting to break into the SCADA of a sewer treatment facility (Lappin, 2011, 143). While terrorists may target infrastructure systems, it is also likely they may target the United States economy as a whole. The purpose would be to launch multiple cyber-attacks with the intention of creating economic instability, plunging the United States into chaos (Rollins and Wilson, 2007, 7). Through wide spread attacks of infrastructure systems in connection to attacks on banking systems or the stock market, it would be possible to plunge the United States into a new recession.

Jihadist organizations, such al Qaeda, have actively embraced the internet as a tool. It has been instrumental in allowing these groups to thrive and communicate in the shadows, while at the same time offering an opportunity to coordinate future attacks. With fewer opportunities to train, coordinate, and indoctrinate followers in physical locations, many now look to the internet for new life (Lappin, 2011, 25). This has given birth to a “virtual caliphate”, where Jihadist’s who look to revive the traditional caliphate system in the real world, have begun

laying the foundation digitally (Lappin, 2011, 25). These online jihadists are very organized, and dozens of websites are dedicated to the regeneration of the caliphate system (Lappin, 2011, vii).

The most immediate threat is the countless websites dedicated to teaching terrorists how to properly operate weapons and build explosive devices (Lappin, 2011, 47). For example these websites teach how to maximize the effectiveness of a car bomb. Websites encourage practices such as loading a car's doors and trunk full of fragments of debris, and then parking near the entrance of a market (Lappin, 2011, 53). This way when the car bomb is detonated, maximum human casualties can be ensured (Lappin, 2011, 53). These websites also teach survival skills and list the equipment necessary for any soldier determined to fight the decadence of the West (Lappin, 2011, 48). Most importantly, these websites educate terrorist on how to plan and execute attacks against both military and civilian targets (Lappin, 2011, 49).

Al Qaeda associated groups; skillfully use the internet to spread their propaganda as well. Sometimes the attempt is to use psychological tactics to spread panic and fear (Lappin, 2011, 64). The internet is a powerful tool to spread dogma and recruit future martyrs. In Iraq for example, insurgents used cyberspace, to not only coordinate attacks against military forces, but they then posted videos of the roadside bombings to recruit new members (Harris, 2009, 19). These online communities existing on the internet increase groupthink and reinforce jihadist dogma and further radicalize individuals (Lappin, 2011, 127). This actually creates more dangerous groups with more extreme beliefs (Lappin, 2011, 124). The only truly effective counter terrorism strategy is one which changes the narrative of potential terrorists and prevents them from filling the ranks of terrorist organizations. This is impossible, as long as terrorist organizations maintain a means to distribute their propaganda and raise funds; they will continue to recruit new members.

Effective counter terrorism cannot simply be a reactive response (Crelinsten, 2009, 235). It must also be proactive and preventative; one of the most important parts of prevention is changing the mentality of terrorist and convincing them to see the value in non-violent ways of achieving their goals (Crelinsten, 2009, 235-236). There is a belief by some that the United States is losing the 'war against cyber-terrorism' by solely focusing on preventing cyber-terrorist attacks. The reason is that the United States is failing to effectively prevent terrorist's primary use of the internet for both communication and indoctrination (Lappin, 2011, 125). This is the equivalent of increasing homeland security efforts, but failing to pursue terrorists abroad in Afghanistan and Pakistan. Terrorism cannot truly be prevented, while terrorists are allowed to strategize and recruit. While there have been increased efforts to monitor terrorist website, it is still difficult to prevent these sites. The reason for this is, when one website is targeted and shutdown, the information and communications on that site simply reappear somewhere else on the internet in a few days (Lappin, 2011, 127).

It is disconcerting that in many cases, the intelligence community has not made the effort to prevent the existence of terrorist websites (Aid, 2012, 178). In fact, only recently has the intelligence community started monitoring these sites, fearing that they may contribute to the growth of terrorist activities against the United States (Aid, 2012, 178). Some within the intelligence community think it is in the best interest of security not to disrupt these communications and websites, but instead allow them to continue as valuable information can be gathered (Rollins and Wilson, 2007, 17). The advantage to this approach is that while the enemy is allowed to plan, coordinate, and spread doctrine; at least it is known what and where they are disseminating information. Monitoring the vast eco-system of cyber-space can be a difficult

task. Since most sites do eventually reappear online, it might be wiser to allow these sites to flourish where they are known, so that they can be monitored and analyzed.

Cyber-Criminals and Cyber-Terrorists

Cyber-crimes currently represent the most prolific cyber-threat; it is more common than acts of cyber-terrorism or the cyber-warfare attacks waged by states. There are many different activities which can be considered cyber-crime, these include: fraud, forgery, intellectual property theft, data system interference, illegal device access, and signal interception (Negroponte and Palmisano, 2013, 23). Financial crimes are growing at an astronomical rate, and during the past decade these cyber-crimes have grown by more than thirty percent in some years (Carr, 2009, 6). These types of crimes may seem completely different from acts of cyber-terrorism, but they are in fact closely connected. One reason is that a decrease in state sponsored terrorism around the globe has forced terrorist organizations to turn to cyber-crime as a means of funding (Rollins and Wilson, 2007, 18). Many terrorist organizations now rely on cyber-crimes like credit card fraud and identity theft to finance their terrorist activities (Lappin, 2011, 98). Organized Crime throughout the world has actively embraced cyber-crime for its profitability (Carr, 2009, 6). Even with law enforcement agencies worldwide adapting to better pursue cyber-criminals, these criminals still face a high probability of success, and a low risk of being caught (Carr, 2009, 6).

Cyber-crimes are also connected to cyber-terrorism in another way. The underground world of cyber-crime is also the developmental 'proving ground' for hackers (Carr, 2009, 5). This is also where the malicious software and command hacks used to cripple computer systems can be developed and perfected (Carr, 2009, 5). In many instance, the hackers who preform cyber-crime, are later recruited to participate in acts of cyber-terrorism. The hackers in Gaza

responsible for launching cyber-attacks against Israel made their living committing cyber-crimes (Carr, 2009, 5).

Cyber-crimes, such as identity theft may in fact be a component of a larger terrorist attack. Back in 2006, the identities of 1500 employees at the National Nuclear Security Administration (NNSA) were stolen (Rollins and Wilson, 2007, 19). The NNSA is the Agency within the Department of Energy responsible for the security of nuclear weapons and nuclear material. It is no secret that al Qaeda, under the leadership of Osama bin Laden, sought fissile material and operational nuclear weapons (Bergen, 2011, 215). It could be possible that stealing the identities of individuals working in the NNSA, the very people responsible for securing both nuclear weapons and nuclear material, was the first step in a larger plan to become the world's first nuclear non-governmental organization. Another disconcerting fact was that this cyber-attack was not detected by officials for more than a year (Rollins and Wilson, 2007, 19). No one really knows what systems may have already been infiltrated and exploited by hackers, and no one may know until it is too late. This is another scary truth of the cyber age; it is difficult to know when exactly a computer system has been breached. The only way to truly prevent hackers is to avert them from ever accessing critical systems in the first place.

Approaches to Security

Many policy makers believe that the cyber-warfare, something the United States has been preparing for decades, is fundamentally different from acts of cyber terrorism (Carr, 2012, 5). This is a fallacy. In fact whether threatened by a nation-state, a terrorist organization, or a rogue hacker, the ability to execute attacks and the types of attacks which can be executed are dramatically similar. More importantly, attacks from all three groups can be mitigated with

improve defensive capabilities. The security measures designed to protect against one set of cyber-attackers will likely protect against another type of cyber-attackers as well.

It seems that the major challenge which has presented itself when trying to evolve the United States' cyber-security abilities and strengthen its cyber-security is an issue of leadership. We still live in a time, when a majority of military commanders were trained in a pre-digital age (Harris, 2009, 20). For this reason, the military has been very slow to adapt to the digital tool that is cyber-space. This is natural as the senior leadership has had trouble rethinking strategies and traditions to embrace the non-traditional methods of warfare (Harris, 2009, 20). A failure to truly understand the digital world in which we live has left the United States vulnerable to attack.

While the military may be slow in adjusting to cyber-threats, the executive branch has been adaptive, just not at the speed which is necessary. The true vanguard of cyber-security has been the Department of Homeland Security (DHS). As the youngest executive department it seems most willing to actively to have embraced cyber-security. The DHS established the Protected Repository for Defense of Infrastructure Against Cyber Threats (PREDICT) as a nexus between the government, the private sector networks, and the cyber-security experts with the intention of sharing research and developing technical solutions (Cellucci, 2011, 395). Within the DHS exists the Office of Cyber-security and Communication, which is tasked with enhancing the nation's cyber-security by engaging both the private sector and our international partners (Cellucci, 2011, 345). The Cyber Education and Workforce Development Program is another brainchild of the DHS, and is designed to help train a competent workforce to meet the network security needs of the world today (Cellucci, 2011, 346). The National Infrastructure Protection Plan (NIPP) was designed to improve infrastructure security and develop appropriate responses

at the federal, state, and local levels (Cellucci, 2011, 32). These are just a few examples of how the DHS has worked to improve cyber-security within the United States.

The intelligence community has greatly expanded their number of personnel and operations, in the decade following the September 11 attack, and now they are an integral part of the nation's cyber-security. Unfortunately, despite the expansion in intelligence efforts, this has made intelligence collection more difficult to manage now than it was prior to the expansion (Aid, 2012, 214). Despite the growth in the number of intelligence agencies, the advancements in computer technology, and an increase in budgets; the major intelligence problem of the Cold War still exists today and that is the lack of intelligence analysts (Aid, 2012, 215). During the Cold War, the United States was able to collect an abundance of information, but it just did not have enough analysts to examine the information effectively and efficiently, nor interpret the information collected. While many collection efforts have indeed gotten better over the last decade, unless the efforts to analyze data improve, the United States will still fall steps behinds its enemies, both state and non-state (Aid, 2012, 215). This is particularly true when considering cyber-terrorists, as only skilled analysts can help detect and prevent acts of cyber-terrorism. The Joint Terrorism Task Force is made up of some eighteen different intelligence agencies; and is tasked with cooperating to prevent cyber-attacks (Kraft and Marks, 2012, 256). This is one way that the intelligence community has been combining resources, and analysts, in an attempt to improve national cyber-security. In 2010, an agreement was reached between the DOD and the DHS to improve coordination between both agencies (Kraft and Marks, 2012, 117). Through the sharing of personnel, both Departments hope to improve communications and better compliment their security objectives (Kraft and Marks, 2012, 117).

The executive branch under Presidents Bush and Obama stepped forward with efforts to improve U.S. cyber-security. The Bush Administration issued a directive which created the Comprehensive National Cyber-security Initiative (Kraft and Marks, 2012, 115). The objectives were to improve awareness of U.S. vulnerabilities, advance counterintelligence capabilities to better defend key information technology, to expand cyber-education programs, and to increase the research and development of new technologies (Kraft and Marks, 2012, 115). The Obama Administration created its own goals for improving cyber-security. These include increasing public awareness and educating the public on the importance of cyber-security (White House, 2009, 14). The President also plans to improve partnerships between the private sector and the federal government to create a responsible and coordinated approach to cyber-space (White House, 2009, 18). The Obama administration also committed itself to developing clear procedures to respond effectively to a large scale cyber-attack on the critical infrastructure (White House, 2009, 24).

These efforts by the government are important, even though they are too basic and backdated. These policies to not emphasize defense nearly enough. The importance of cyber-security is not emphasized enough in the United States. Every computer system – public, private, personal - should be protected, at a basic level with firewalls and antivirus software; these are the only surefire ways to prevent low level computer worms and Trojan horses (Lappin, 2011, 110). However, software and firewalls only protect against what they already know, and are told to guard against. One option to securing the internet which the government could explore is having internet service providers introduce software to clear web traffic as it goes through networks, in order to detect malicious and threatening software faster (Lappin, 2011, 110-111). The government currently requires public utilities, like water, to be purified and treated to ensure

customers receive safe water (Lappin, 2011, 110-111). Maybe internet traffic should be purified in a similar spirit to ensure a safer internet?

Optimists believe that an international treaty is the only way to secure the internet. The Obama administration even supports the idea of greater international cooperation to securing cyber space (White House, 2009, 20). Considering the rapid development of computer technologies and information systems, cyber-warfare is the natural evolution of defense. Some argue that it is necessary and logical to regulate these new and destructive weapons. Arms control treaties have been successful in the past; and have for decades worked to regulate the movement of nuclear material and remove biological and chemical weapons from international conflict. A digital arms treaty could define the types of cyber-attacks which are acceptable in the modern world. Ironically enough, the biggest support of an international treaty on cyber-space has been the Russian Federation (Clark and Knake, 2010, 219). Russia has introduced a number of cyber treaties calling for the regulation of cyber-attacks between nation states.

The United States has been adamantly opposed to international attempts to create a digital arms treaty (Clark and Knake, 2010, 219). The belief of the United States is that cyber-warfare treaties are counterproductive until the cyber battlefield is better understood and until practical verification methods can be created (Clark and Knake, 2010, 220). Verification is an important component of arms control. Only after verification became possible, were the superpowers able to reach agreements on nuclear weapons during the Cold War. Part of what makes cyber verification difficult, is each nation has a vastly different digital infrastructure. For example, Estonia and South Korea provide the greatest access to broadband internet; the United Arab Emirates has the greatest access to mobile internet devices, while the United States has the

greatest dependency on a networked infrastructure (Clark and Knake, 2010, 226). Every nation is technologically different, thus has different abilities and vulnerabilities within cyber-space.

While the United States does oppose an agreement regulating cyber-space and cyber-warfare; it does support international agreements to coordinate and assist in preventing cyber-crimes and cyber-terrorism. This is one of the ways the Obama administration does support international cooperation in cyber-space. More than forty nations worldwide signed onto the Budapest Convention on Cyber-Crime, a cyber-treaty to establish an international baseline for regulating cyber-space and assisting with the prosecution of cyber-criminals (Negroponte and Palmisano, 2013, 23). Unfortunately, some of the most advanced cyber actors – Russia and China - have yet to agree to the terms of this agreement (Negroponte and Palmisano, 2013, 23). In the case of Russia, it seems unlikely that they will support such a treaty which they believe violates their sovereignty (Carr, 2012, 171). While each nation does have a right to protect its national sovereignty and to remain free from foreign intervention within its own borders, that failure of Russia to join this international agreement is problematic. It gives life to cyber-terrorist, by providing them shelter within Russia. It is still highly likely that many of these potential terrorist will be interested in attacking Russia, especially if they reside in Chechnya or Ingushetia, but the presence of cyber-terrorists anywhere in the world is a potential threat to the United States. It is ironic that Russia, a nation that supports a treaty on cyber-warfare, does not want to support a treaty on cyber-crime.

The white-elephant in the discussion of cyber-security for the past few months has been the NSA. The NSA claims that it has prevented nearly fifty-five terrorist attacks around the world (Kelly, 2013). Not everyone agrees with these claims, believing that the NSA is simply trying to over justify its actions (Poulsen, 2013). The NSA has not just become the favorite target

of policymakers on the Hill, but those throughout the country as well. In the California Senate, legislators on both sides of the aisle are pushing legislation to prohibit the State from contracting with companies that contract with the NSA (Nelson, 2014). This legislation would also outlaw NSA partnerships and research at State Universities, and prohibit construction of NSA facilities in California (Nelson, 2014).

The President has recently been presented with some forty recommendations on how to scale back the powers of the NSA (Pace and Dozier, 2014). The recent actions have the NSA have brought forth a whole set of issues, which threaten the future of digital surveillance and cyber security. The United States is facing a national security crisis. Which organization will become the cyber-security vanguard, monitoring the cyber-terrorist worldwide? Will the United States successfully maintain its ability to successfully monitor cyber-terrorist worldwide? The NSA acknowledges that in the wake of Snowden's revelations, and the looming organizations changes, the ability to successful protect the nation cyber-terrorists is questionable (Kelly, 2013). The only practical option for the United States intelligence community is to dedicate more efforts to improving cyber-security. If collection methods recently called into question are to be eliminated, this could inhibit the ability to successfully prevent terrorist attacks, both conventional and digital. The only practical option for protecting critical infrastructure is to improve security measures. For this to happen, the burden of cyber-security will have to pass from Executive Agencies to the United States Congress.

Apprehensive hackers point to events like the 2003 blackout which affected portions of both the United States and Canada, as an example of the devastating potential of a cyber-attack (Crelinsten, 2009, 168). The failure of the power grid affected the systems controlling water, transportation, manufacturing, and communications (Crelinsten, 2009, 168). They believe that an

intentional cyber-attack on critical infrastructure within the United States will result in widespread chaos and destruction. The San Diego Blackout of 2011 is evidence of this. Sand Diego was essentially brought to a standstill through the loss of power at a critical juncture (Gustafson, 2011). Nearly 5 million were effected when power failed to schools and business, traffic signals and the airport became dysfunctional (Gustafson, 2011).While they are right about the results of such an attack, the threat of a cyber-attack on infrastructure does not seem as immediate as many hackers believe.

Yes, protections on critical Infrastructure need to be dramatically improved. Two years ago, the DHS reported that cyber-attacks targeting critical infrastructure had risen by 383 percent from the previous year (Negroponte and Palmisano, 2013, 18). That is a harrowing statistic, showing how the security of such infrastructure systems needs to be updated. As the number of cyber-attacks increases, so does that probability that one of those attacks will be successful. While the many terrorist organizations worldwide have yet to succeed in initiating a large scale cyber-attack, it only seems to be a matter of time before they possess the capabilities to. At the same time, many smaller nations around the world are also improving their own cyber abilities. While it seems the United States is not immediately threatened by an infrastructure cyber-attack, defensive measures need to become a priority sooner rather than later. Computers are too widely available, and there are too many actors investing time and money into perfecting their offensive cyber-abilities to continue to approach our cyber-security with a lackadaisical attitude.

Isaac Asimov did not fear computers, but Isaac Asimov lived in a time before computers were tasked with such extraordinary responsibilities. Maybe he is right, and policy makers should not fear computers, but policy makers do need to fear the individuals using computer with malicious intentions. Perhaps instead of fearing computers, we should recognize the valuable and

irreplaceable role they play in society. Cyber-security efforts need to be improved, to make sure the computers we rely upon are safe and secure. Without improved defensive measures, we will not be able to continue living the lives we have grown accustom to for much longer.

REFERENCES

Aid, M. M. (2012). *Intel wars: The secret history of the fight against terror*. New York, NY: Bloomsbury Press.

Bergen, P. L. (2011). *The longest war*. New York, NY: Free Press.

Carr, J. (2012). *Inside Cyber Warfare* (2nd ed.). Cambridge, UK: O'Reilly.

Cellucci, T. A. (2011). *A guide to innovative public-private partnerships*. Toronto, Canada: The Scarecrow Press.

Clapper, J. R. (2013, April 18). 2013 National Intelligence Threat Assessment. In *Director of National Intelligence*.

Clark, R. A., & Knake, R. K. (2010). *Cyber war*. New York, NY: HarperCollins.

Collins , J., & Wilson, C. (2007, January 22). Terrorist capabilities for cyber-attack: Overview and policy issues. [Electronic version]. *Congressional Research Service: Report for Congress*, 1-28.

Crelinsten, R. (2009). Counterterrorism. Cambridge, UK: Polity.

Goldman, D. (2013, January 9). Hacker hits on U.S. power and nuclear targets spiked in 2012. In *CNN Money*. Retrieved April 3, 2014

Gustafson, C. (2011, September 8). Unprecedented outage left millions in the dark. *The San Diego Union Tribune*. Retrieved April 1, 2014

Harris, S. (2009, November 14). The Cyber-war plan. *National Journal*, 19-25.

Kelly, H. (2013, August 1). NSA chief: Snooping is crucial to fighting terrorism. In *CNN Tech*. Retrieved January 4, 2014

Kraft, M. B., & Marks, E. (2012). *U.S. Government Counterterrorism*. New York, NY: CRC Press.

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and national security*. Washington, D C: Center for Technology and National Security Policy.

Lappin, Y. (2011). *Virtual Caliphate*. Washington, DC: Potomac Books.

Nelson, S. (2014, January 7). California Legislators introduce bill to banish NSA. In *U.S. News*. Retrieved January 7, 2014.

Negroponte, J. D., & Palmisano, S. J. (2013). *Defending an Open, Global, Secure and Resilient Internet* (Vol. 70). New York, NY: Council on Foreign Relations.

Pace, J., & Dozier, K. (2014, January 9). Lawmakers: Obama weighing changes in NSA Policy. In *ABC News*. Retrieved January 9, 2014

Poulsen, K. (2013, December 16). 60 Minutes puff piece claims NSA saved U.S. from cyberterrorism. In *Wired*. Retrieved January 7, 2014.

Rollins, J., & Wilson, C. (2007, January 22). Terrorist capabilities for cyber-attack: Overview and policy issues. Congressional Research Services.

Shea, D. (2004, January 20). Critical infrastructure: Control systems and the terrorist threat [Electronic version]. *Congressional Research Service: Report for Congress*, 1-22.

Sweetman, B. (2009, November). H4XOR3D! Means hacked. *Defense Technology International*, 30-31.

White House (2009) *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*.

White House. (2010). *National security strategy.*