ARE CONGRESSIONAL ACTIONS AND EXECUTIVE CYBER POLICY DIRECTIVES SUCCESSFUL IN THE POST 9/11 ERA?

Alee Corrales
Texas A&M University-Commerce
Department of Political Science
acorrales2@leomail.tamuc.edu

Abstract: Following the September 11th terror attacks in New York City and Washington, D.C., policymakers in the United States began placing a stronger emphasis on cybersecurity and terror prevention. Due to the rapidly changing nature of cybersecurity, it was difficult to quickly address all the cybersecurity threats looming over the United States. Early efforts to improve cybersecurity included the establishment of the Department of Homeland Security to organize cyber threat data across various agencies. Several pieces of data-sharing legislation were circulating through Congress at this time, as well. Soon after, the U.S.A. Patriot Act became law. President Obama prioritized cybersecurity during his administration, and President Trump is prioritizing the issue, as well. This research paper finds the aforementioned policies implemented after the 9/11 attacks to be successfully detecting online communication between terrorist actors and protecting the cybersecurity interests of the United States.

INTRODUCTION

Protecting the national security interests of the U.S. is vital to the nation's well-being and prosperity. Considering the U.S. is the leading military superpower in the world, it is no surprise that efforts to improve national security are always sought after. In recent decades, a new breed of national security threat has risen: cyber-assisted terror attacks, cyberwarfare and cybersecurity vulnerabilities. Cybersecurity is a rapidly changing field; when less technology existed, cybersecurity was less of an issue. However, the technological advances made over the past decades are wildly apparent, and the cybersecurity dilemmas that accompany these technological developments are apparent, as well. National security experts and policy makers are constantly looking for methods to thwart terror attacks and detect terror activity. The biggest terror attack in U.S. history occurred on September 11th, 2001, when two airplanes bombed the World Trade Center buildings in New York City. This terror attack was a wake-up call for policy makers in the U.S.

After the 9/11 terror attacks, policy makers scrambled to address the errors that allowed the attack to occur. Due to the fact elements of this attack were enabled through online communication, and some of the terrorists perpetrating the attack could have been discovered through surveillance of online communication, there has been a dramatic shift in online surveillance practices and policies since the 9/11 terror attacks. This research paper will examine the quantity of cybersecurity policy before and after the 9/11 attacks, what types of cybersecurity policies were implemented, which lawmakers lead efforts to change cybersecurity policy, and whether or not the policies implemented have proven successful. The main question is, from a cyber policy standpoint, how did the U.S. respond to the 9/11 terror attacks? The establishment of the Department of Homeland Security, data-sharing legislation in Congress, Executive Orders regarding cybersecurity, and the Patriot Act will be the key policies analyzed in this paper.

For the sake of clarity in the upcoming pages, there are a few definitions that should be noted prior to the cyber policy discourse herein. According to U.S. Code Chapter 6 Subchapter 1501, a *cybersecurity threat* is defined as "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system" (U.S. Code 2013). Likewise, *cyberwarfare* is defined in the *Oxford English Dictionary* as "The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes" (*Oxford English Dictionary* 2013) Similarly, *cyber policy* will be regarded as any legislation or executive directive relating to cyberwarfare, and/or cybersecurity as defined above.

One important aspect of cybersecurity that must be noted is that it has radically changed as technology has increased. According to Herman Tavani, author of *Ethics and Technology: Controversy, Questions, and Strategies for Ethical Computing*, there are four stages of cyber technology, and the U.S. is currently in Phase 4, "a point at which we have begun to experience an unprecedented level of convergence of technologies" (Tavani 2016, p. 8). Many aspects of technology are becoming homogenous to activities in daily life. Because of this, the issue of cybersecurity has substantially changed and expanded in recent years. For example, according to the North Atlantic Treaty Organization (NATO), the first major cybersecurity breach in the U.S. occurred in 1988, when the Morris Worm, "one of the first recognized works to affect the world's nascent cyber infrastructure," spread through computers all over the U.S., finding and duplicating UNIX software vulnerabilities (NATO 2013). Following this attack, and many others, NATO began taking cybersecurity efforts more seriously. According to Glenn Crowther, author in the *Cyber Defense Review*, both NATO and the Department of Defense (DoD) now recognize cyber as "a 'domain,' co-equal with air, land, and sea" (Crowther 2017, p. 63) The Morris Worm was the first of many cybersecurity breaches, which subsequently occurred on a domestic and international level.

The Morris Worm was not intended to commit any criminal or terroristic attack, but many of the following viruses and breaches were more destructive in nature, with many of them stealing or compromising data - impacting the national security of various nations. The next major data integrity breach occurred when "hundreds of networks belonging to NASA and several other U.S. government agencies" were compromised through several coordinated attacks (*MIT Technology Review* 2015). After the attack, one investigation by the SANS Institute found "that the attacks originated in the Chinese province of Guangdong and were probably the actions of Chinese military hackers" (*MIT Technology Review* 2015, pp. 12). This attack was one of the first solely-cyber, malicious attacks committed against the U.S. by a foreign government. At this point, it is clear that governments are beginning to utilize cyber technology for military/ intelligence gathering purposes. Additional and more recent examples of cybersecurity breaches will be discussed throughout this paper.

Online Communications and September 11th

As technology rapidly increases on a domestic and international level, cyber-related crime has drawn much interest from the U.S. government. In the largest terror event in U.S. history, the

September 11th attacks, online communication occurred between various terrorist operatives involved in the attack. According to *CNN*, al-Qaeda, the Islamic terrorist organization that committed the attack, “uses Web sites and e-mail addresses in Turkey, Nigeria and tribal areas of Pakistan to pass messages among themselves” (Arena and Bohn 2004). This is an example of a cyber-related crime, because the terror attack was not executed online or in cyberspace, but the terrorists were aided by online communication. Hence, the U.S. government decided to increase internet surveillance in order to thwart future terror attacks.

Although not the topic of this paper, the increased surveillance of internet communication, which is done in order to detect terrorist/criminal activity, is causing significant privacy issues. The National Security Agency (NSA) is the primary organization being scrutinized for its surveillance practices. According to *The New York Times*, “The National Security Agency vacuumed up more than 534 million records of phone calls and text messages from American telecommunications providers like AT&T and Verizon last year” in order to search them for potential terror-related communication (Savage 2018, pp. 1). Many individuals are skeptical of this surveillance, which is proving to be one of the most prominent domestic issues related to national security and cyber-assisted warfare. The U.S.A. Patriot Act*,* is one piece of legislation regarding government surveillance of online communication - it will be discussed later on. What is important to understand is al-Qaeda and its affiliates did, indeed, communicate on the internet and used this communication to help carry out their attacks on September 11th. This attack spurred a new era of policies intended to detect and thwart terrorist activity, cyberattacks, and allow for better data sharing between agencies involved with law enforcement and national security.

CONGRESSIONAL ACTION AND EXECUTIVE DIRECTIVES REGARDING CYBER POLICY

One of the first changes made on the federal level after 9/11 was the establishment of the Department of Homeland Security. This recommendation was brought forth by the 9/11 Commission, a bi-partisan commission directed to analyze the events and causes that led to the 9/11 attacks and to "provide recommendations to guard against future attacks" (9/11 Commission 2004). Therefore, when the commission recommended the Department of Homeland Security (DHS) be established, the recommendation was taken seriously by Congress. In 2002, towards the end of the 107th Congress, Representative Richard Armey from the 26th Congressional District of Texas introduced the Homeland Security Act of 2002, H.R. 5005 (Armey 2002). This bill was introduced to establish DHS as an executive agency, with the agency's secretary being appointed by the President and confirmed by the Senate (Armey 2002). The bill was signed by President George W. Bush and became law in November, 2002. DHS's goal, to this day, is to prevent terrorist attacks in the U.S., reduce U.S. vulnerability to acts of terrorism, and minimize the potential damage that could result from any terrorist act that does occur domestically (Armey 2002). The agency's role is broad, but they immediately recognized the necessity to address the cyber vulnerabilities in the U.S.

In 2009, DHS established the National Cybersecurity and Communications Integration Center (NCCIC), which seeks to analyze and organize the vast amounts of international and domestic cyber threat data as well educate the public regarding these threats (DHS 2009). Soon after, in the 113th Congress, Senator Thomas Carper, a U.S. Senator from Delaware, introduced the National Cybersecurity Protection Protection Act of 2014, S. 2519. This legislation established the NCCIC, which allowed the sharing of cybersecurity risk information between federal and non-federal entities in order to better address potential cyberattacks (Carper 2013). The bill was signed by President Obama and became law in December 2014. The NCCIC proposed by the bill was exceedingly crucial; many post-analysis reports of the 9/11 attacks attributed the apparent intelligence failure, in part, to the fact the CIA, FBI, and NSA were not sharing data with each other, and these federal agencies were also not sharing data with state and local law-enforcement agencies (9/11 Commission 2004). This is commonly referred to as an *information sharing failure,* and it is tragic to imagine what could have been prevented if federal and state agencies were in better communication before the 9/11 attacks. This bill could prevent the same failure from occurring in the future, because the goal of the NCCIC is to organize and analyze cyber threat data from all agencies at the federal, state, and local level of government. According to Timothy Goines in *Strategic Studies Quarterly,* "using an interagency coordination process, the United States will be better positioned to employ an effective cyber deterrence policy" (Goines 2017, p. 86).

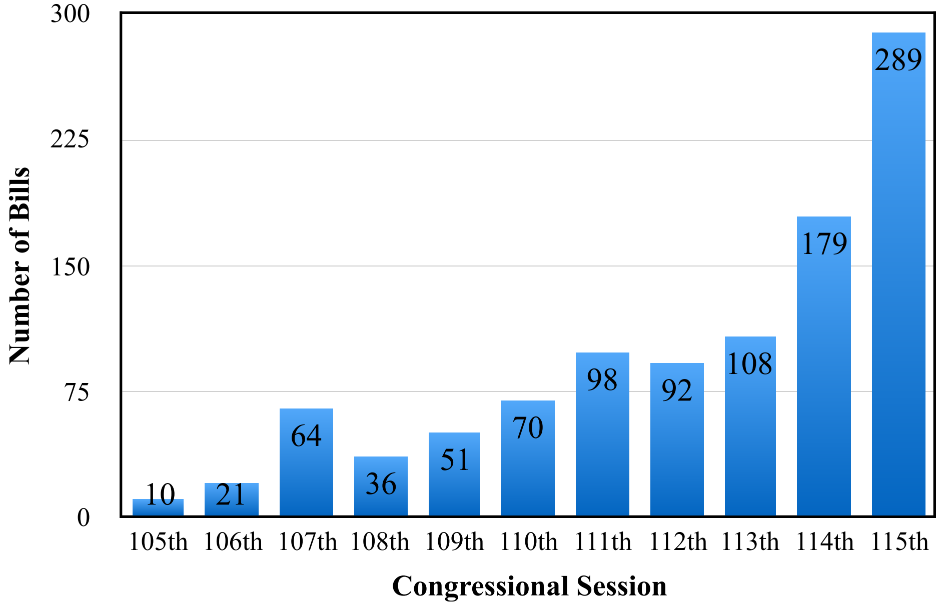
Another key piece of cyber legislation is H.R. 3619, Coast Guard Authorization Act of 2010, which Representative James Oberstar, a congressman from Minnesota, introduced in the 111th Congress. This legislation is very broad, but Section 202 must be noted. The bill "Authorizes Coast Guard industrial activities to accept orders and enter into agreements with establishments, agencies, and departments of the Department of Defense (DoD) and the Department of Homeland Security (DHS)" (Oberstar 2010). This was the beginning of a vital relationship between the U.S. Coast Guard (USCG) and DHS. The USCG collects biometric data (i.e. fingerprints, retinal scans) on persons outside the U.S. who could be potential terrorist or criminal threats. Because of the data sharing agreement between the USCG and DHS, when an individual is screened for entry to the U.S., this biometric data is used to authenticate who the individual is and link them to their past, which helps ensure a terror or criminal suspect cannot easily gain entry to the U.S. This data sharing agreement was codified in U.S. Code Chapter 701, Subchapter 1, which reads that the Secretary of the USCG shall oversee the biometric identification of suspected individuals in coordination with DHS (U.S. Code 2010). This is another fascinating example of the importance of technology and data sharing in national security.

Additionally, the U.S.A. Patriot Act falls in the discussion of cyber policy and should be considered in context of the 9/11 attacks. H.R. 3162, The U.S.A. Patriot Act (referred to hereafter as the Patriot Act), was introduced in the 107th Congress by Representative James Sensenbrenner from Wisconsin. The Patriot Act was signed by President George W. Bush and became law in October 2001. This legislation illustrated the broad anti-terror sentiment in the U.S. immediately after the 9/11 attacks. It encompassed everything from establishing the Counterterrorism Fund to expanding presidential power under the International Emergency Powers Act (Sensenbrenner 2001). However, the element of this policy that is important to this cyber policy discussion is the "Enhanced Surveillance Procedures" provision, found in Title II, Section 201 and 202 of the law. This provision amended U.S. Code to give the federal government "authority to intercept wire, oral, and electronic communication relating to computer fraud and abuse offenses" (Sensenbrenner 2001). As was mentioned earlier, the NSA has recently been under incredible scrutiny due to their surveillance practices. Analysis of the Patriot Act will continue throughout this paper.

In the aftermath of 9/11, several pieces of cyber legislation were introduced and passed in Congress immediately after the attacks. The 9/11 attacks demonstrated the need for bolstered cyber capabilities in order to protect national security. Today, cyber legislation is being introduced and passed in quantities higher than ever before. For example, the 115th Congress, which occurred 2017-2018, passed several notable pieces of cybersecurity legislation. Representative John Ratcliffe, representing the 4th Congressional District of Texas, introduced H.R. 1616, Strengthening State and Local Cyber Crime Fighting Act of 2017. This bill amends current law to authorize the Computer Forensics Institute, which educates the public regarding prevention of cybercrime, and it also educates state and local law enforcement officers regarding methods to detect and thwart cybercrime on a local level (Ratcliffe 2017). President Trump signed this bill on November 2, 2017, and the resolution became law. Representative Ratcliffe is Chairman of the Cybersecurity and Infrastructure Protection Subcommittee in the U.S. House of Representatives, and it is critically important that he continues to demonstrate the importance of cybersecurity and its implications to national security.

Interestingly, the aforementioned examples of cyber policy are only a minute segment of the cyber policy proposed since the 9/11 attacks. Figure 1 illustrates the number of cyber-related pieces of legislation introduced in Congress over the past two decades. In order to understand the graph, it should be noted the 105th Congress occurred 1997-1998, the 106th occurred 1999-2000, the 107th occurred 2001-2002, the 108th occurred 2003-2004, and this pattern continues in two year increments. Thus, the 9/11 attacks occurred towards the middle of the 107th Congress.

Figure 1: Cyber Legislation Introduced in Congress

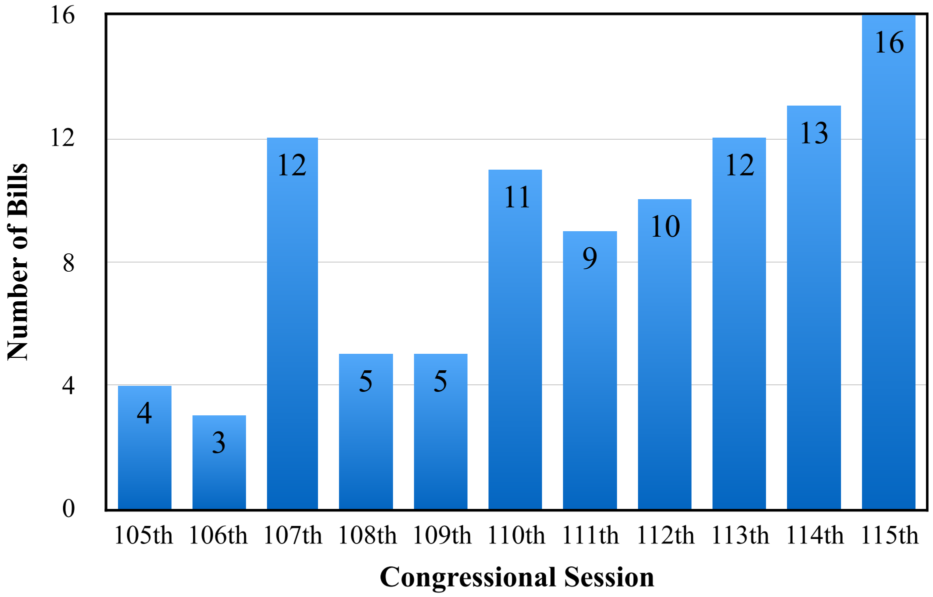


Data compiled by Alee Corrales (2019).
Data retrieved from www.congress.gov.

Using Figure 1, the increase in cyber legislation introduced in the 107th Congress is clear. Several of the cyber-related bills introduced in the 107th Congress were discussed above, the most critical being the Homeland Security Act of 2002. Figure 2 illustrates the cyber-related legislation introduced in Congress that became law. The pattern is almost identical - a clear uptick in cyber-related legislation that became law occurred in the 107th Congress. The Coast Guard Authorization Act of 2010*,* discussed above, became law during the 107th Congress, along with the Homeland Security Act of 2002.

Similarly, there is a clear upward trend beginning in the 111th Congress, which occurred at the start of President Obama's administration. The Obama Administration heavily prioritized cybersecurity and cyber infrastructure. According to Kevin Newmeyer in *PRISM* (National Defense University's Strategic Studies Journal), one of President Obama's first presidential acts was calling for a "comprehensive review of U.S. policy on cybersecurity" (Newmeyer 2012, p.

Figure 2: Cyber Legislation That Became Law



Data compiled by Alee Corrales (2019).
Data retrieved from www.congress.gov.

115). This would explain the increase in cyber-related legislation when President Obama took office.

The United States is notorious for their proactive defense and national security measures. But, following the attacks on 9/11, there were obviously significant changes that needed to be made. With the 9/11 attacks occurring over seventeen years in the past, the DoD and accompanying presidential administrations have continued the efforts to improve cybersecurity in the U.S. and remain current on new types of warfare and weapons. Recently, as shown throughout this paper, cyberwarfare has proven to be tremendously important. In order for the U.S. to remain an indomitable military superpower, they will have to demonstrate that their cyber tactics are equally potent to their physical warfare tactics.

In order to clearly define their cyber guidelines, the DoD established a new five pillar cyber strategy in 2015. The pillars are as follows:

> 1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
> 2. Defend the DOD information network, secure DOD data, and mitigate risks to DOD missions;
> 3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
> 4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages; and
> 5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability (Lange 2018, p. 5).

This strategy is suitable because, it prioritizes defense, but the fourth and fifth pillars also provide leeway to exercise offensive strategies. As will be demonstrated later in this paper, the U.S. has engaged in proactive cyberattacks in order to gather intelligence, prevent terrorist activities, and aid our allies.

Following the publication of DoD cyber guidelines, President Trump decided to establish a clear cyber framework for his presidential administration, which demonstrated his attentiveness to cybersecurity and the role it plays in national security. The Trump Administration established the following four pillars:

> 1. Protecting the American people, the homeland, and the American way of life by safeguarding networks, systems, functions and data.
> 2. Promoting American prosperity by nurturing a secure, thriving distal economy and fostering strong domestic innovation.
> 3. Preserving peace and security by strengthening the ability of the U.S., it partners and allies to deter and punish those who use cyber maliciously.
> 4. Advancing American influence to extend the key tenets of an open, interoperable, reliable and secure internet" (Scheider, 2018, pp. 4-9).

This strategy aims to guide the cyber operations of U.S. military, defense, and intelligence agencies. Likewise, on August 18, 2017, President Trump signed an executive order directing the status of the United States Cyber Command (referred to as Cybercom) be elevated to a Unified Combatant Command (Trump 2017, pp. 1). Cybercom is home to the Army Cyber Command, the Tenth Fleet Naval Cyber Command, the Twenty-Fourth Air Force Cyber Command, and the Marine Corp Cyberspace Command (U.S. Cyber Command 2018). Each of these military service branches offer cyberthreat intelligence and analysis relevant to their branch's current mission. According to the statement made by President Trump, elevating the status of Cybercom would "strengthen our cyberspace operations and create more opportunities to improve our Nation's defense" and "help streamline command and control of time-sensitive cyberspace operations by consolidating them under a single commander" (Trump 2017). This order by President Trump allows Cybercom Commander General Paul Nakasone, who is also the director of the NSA, to pursue limited military actions when a cyberthreat arises. President Trump's elevation of Cybercom is important because it demonstrates the U.S. understands the significance cybersecurity and protecting its citizens from cyberwarfare.

In addition to the executive order discussed above, President Trump also extended one of President Obama's executive orders from 2015. Executive Order 13694, National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, declared a state of emergency to "deal with the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States constituted by the increasing prevalence and severity of malicious cyber−enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States" (Trump 2018). President Trump simply agreed that the U.S. is, indeed, still in a state of emergency due to malicious cyberattacks committed by people and governments outside the U.S.

SUCCESS AND FAILURE IN CONTEMPORARY CYBER POLICY

The goal of updating legislation and issuing new directives is to protect the U.S. from cyber threats, protect U.S. cyber infrastructure, increase information sharing between various agencies in order to improve cybersecurity efforts, and detect terrorist and/or criminal communications online. So, how effectively has DHS managed cybersecurity efforts? Have they prevented any terror attacks or detected online communication between terrorists? Was the Patriot Act an effective surveillance tool for federal agencies? This section will seek to explain the failures and successes of the major cyber policies implemented after the 9/11 attacks.

Although not the fault of DHS, there was one major failure relating to secure cyber threat infrastructure on a national level. While government agencies work together to deter and detect cyber threats, initiating relationships between government agencies and privately-owned firms is far more difficult. Several years ago, the Cybersecurity Act of 2012, S. 2105, was introduced in the Senate by Senator Joseph Lieberman. The text reads as follows: “the private sector is responsible for enhancing security of the nation’s most critical infrastructure while the government ensures effective oversight and compliance” (Lieberman 2012). If the bill passed, the aforementioned “oversight” would have been conducted by DHS and DoD. According to Larry Clinton in the *Journal of Strategic Security*, privately-owned firms were displeased with this bill because “the idea that the private sector would fund national defense needs . . . was both naive and impractical” (Clinton 2015, p. 55). Therefore, DHS waited for a better solution to the issue of government-private partnerships. According to Clinton, the solution came when President Obama issued Executive Order 13636: Improving Critical Infrastructure - Cybersecurity (Clinton 2015, p. 56). This Executive Order utilized a voluntary approach to government-private partnerships, offering private firms who participated in such partnerships tax incentives and grants (Clinton 2015, p. 56). The partnerships developed between private firms and DHS/DoD as a result of this policy experienced huge success regarding of cyber threat prevention and risk management. This partnership is part of the solution to the information sharing failure that occurred prior to the 9/11 attacks.

The Patriot Act has been partially responsible for many foiled terror attacks in the U.S. According to a report from the Terror Analytics team at the Heritage Foundation, "at least 50 publicly known terrorist plots against the United States have been thwarted since 9/11," and this high prevention rate was, in part, made possible by the surveillance tools made available by the Patriot Act (Bucci, Carafano, and Zuckerman 2016). For a visual explanation of the terror attacks that have been thwarted since 9/11, see Figure 3 below. It is important to note that the graph accounts for all foiled terror attacks in the U.S. since 9/11, not just the attacks that were thwarted

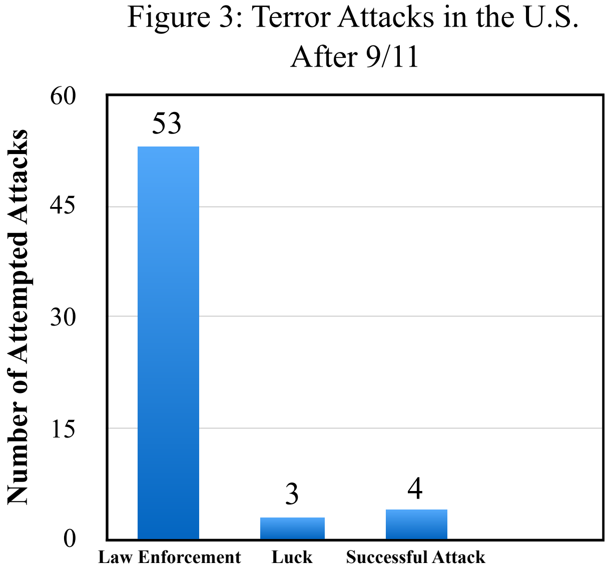


Figure 3: Of the dozens of terror plots against the U.S. since September 11th, 2001, 53 were foiled by law enforcement, 3 were foiled by luck and four were successful.

Data compiled by Alee Corrales (2019).
Data Retrieved from the Heritage Foundation (2016).

due to cyber policy changes. However, it does offer insight into how well all the policies implemented after 9/11 are working holistically.

In 2004, former FBI Director Robert Mueller testified before the Senate Judiciary Committee and said “the PATRIOT Act has proved extraordinarily beneficial in the war on terrorism and has changed the way the FBI does business . . . Many of our counterterrorism successes in fact, are the direct results of provisions included in the Act” (Mueller 2004). He continued to say that without the U.S.A. Patriot Act, the FBI would be mandated to revert back to pre-9/11 antiterrorism efforts, which were, unfortunately, flawed (Mueller 2004). One example of the FBI successfully using surveillance techniques occurred in July 2006 when Assem Hammoud, an al-Qaeda loyalist, was planning a terror attack in New York City. Because of their increased surveillance capabilities under the Patriot Act, the FBI detected the online communications regarding the attack and stopped if from happening. Hammoud was convicted and imprisoned in Lebanon (Bucci, Carafano, and Zuckerman 2016). Similarly, in February 2011, the FBI discovered potential terror targets in Texas through surveillance of Khalid Ali-M Aldawsari’s email (Bucci, Carafano, and Zuckerman 2016).

Former NSA Director Keith Alexander testified before the House of Representatives saying over 50 terror attacks were thwarted due to NSA surveillance programs made possible by the Patriot Act (Bucci, Carafano, and Zuckerman 2016). Therefore, the surveillance provisions in the Patriot Act did offer federal agencies the necessary tools to stop numerous potential terror attacks.

Offensive Cyber Strategies Incorporated into U.S. Intelligence Efforts

According to James McGhee in *Strategic Studies Quarterly,* "offensive cyber operations are increasingly an important part of our national defense and provide commanders with unique capabilities to thwart enemy attacks" (McGhee 2016, p. 46). After discussing the 9/11 attacks and policies resulting from the attacks, one might wonder if the U.S. has ever employed cyberwarfare as an offensive military tactic. Indeed, the U.S. has incorporated cyber strategies into many of its intelligence gathering and anti-terror strategies. The first example is the Stuxnent computer worm first identified in 2010. Stuxnet is "an extremely sophisticated computer worm that exploits multiple previously unknown Windows zero-day vulnerabilities to infect computers and spread" (Fruhlinger 2017, pp. 1). This virus was intended to defray the capabilities of computer systems involved in uranium enrichment and its first documented appearance was in Iranian nuclear facilities. The virus was extremely complex and — when Stuxnet infects a computer, it connects to programmable logic controllers (PLCs), alters the PLCs programming, which results in uranium centrifuges spinning too quickly, ultimately destroying several components of the centrifuge operation (Fruhlinger 2017, pp. 1).

Interestingly, the Stuxnet worm exploited vulnerabilities on Windows computers not connected to the internet. However, it is reported that one employee at an Iranian nuclear facility brought a laptop home after he left the facility, connected the laptop to the internet, and, albeit unintentionally, allowed the worm to spread online (Fruhlinger 2017, pp. 12). Although no government formally took responsibility for the production and use of Stuxnet, deductive reasoning points to two probable entities. The Middle East is a highly tumultuous area where Western democracy and practices often garner disapproval. The U.S. is highly Westernized, and the nation of Israel is the closest U.S. ally in the Middle East. Due to strong distaste for the U.S. and Israel, there is speculation that a nuclear capable Iran could have devastating effects for Israel, and potentially for the U.S., as well. Therefore, the governments plausibly responsible for the Stuxnet attack are, the U.S. and Israel (Fruhlinger 2017, pp. 4).

In addition the Stuxnet worm, another impressive U.S. cyberattack occurred in 2013 when the sources discovered the U.S. hacked “Chinese mobile phone companies to collect text messages and spied on the Tsinghua University,” which is a premier research university in China (Rapoza 2013, pp. 1). According to Edward Snowden, a former NSA and Defense Intelligence Agency employee, the U.S. had been spying on Chinese citizens for years (Rapoza 2013, pp. 2). This surveillance program, widely known as PRISM, is fascinating because it was used to conduct a data breach in China, but, the PRISM program is used domestically for surveillance of U.S. citizens, as well. According to Matthew Croston in *Strategic Studies Quarterly*, the U.S. must take an increasingly proactive approach to cyberstrategy in order to continue competing with and deterring China (Crosston 2012, p. 101). This surveillance program exemplifies the ability of the U.S. to carry out offensive cyber strategies.

CYBERWARFARE SHIFTING GLOBAL DYNAMICS

Interestingly, while cyberwarfare has some similarities to war in the physical realm, it also has a few key differences. According to an article in the *California Law Review*, cyberwarfare has become common in recent years and is capable of dismantling nuclear centrifuges, air defense systems, and electrical grids, but, “the attacks look little like the attacks the law of war has traditionally regulated” (Hathaway et al. 2012, p. 820) For example, cyberwarfare levels the field between large and small countries, because executing a cyberattack does not require as much military personnel as a physical attack does. In the previously discussed Stuxnet attack in Iran, a reporter for the The Institute of Electrical and Electronics Engineers estimated that a team of ten programmers wrote the C++ code used to execute the attack (Kushner 2013, pp. 20). This worm, as mentioned above, damaged the uranium centrifuges at an Iranian nuclear power plant (Fruhlinger, 2017, pp. 1). Imagine if the same operation, disabling centrifuges, was carried out physically with soldiers invading the power plant. Such a hypothetical operation would dictate a large support team and would risk people's lives. However, the Stuxnet worm, written by ten programmers, still inflicted significant damage to the centrifuges. Thus, cyberwarfare could potentially allow nations with less manpower and other resources to carry out effective military action through cyber capabilities.

Another aspect of cyberwarfare to consider is that it magnifies tensions between rival countries. The top state actors posing cybersecurity threats to the U.S. are Russia, China, and North Korea (Olenick 2017, pp. 1-5). Each of these countries have carried out varying levels of cyberattacks against the U.S. and citizens therein. Russia's cyberattacks include the Democratic National Committee and Yahoo, North Korea's cyberattacks include Sony Entertainment and the Society for Worldwide Interbank Financial Telecommunication, and China's cyberattacks include the U.S. Office of Personnel Management and the Federal Deposit Insurance Corporation (Olenick 2017, pp. 5-9). While these attacks may not appear damaging, they actually did cause substantial privacy breaches and result in the compromise of numerous federal documents. According to the book *The U.S. China Military Scorecard*, in regards to potential cyber conflicts between the U.S. and China, "the U.S. brings a much better foundation to the battle than does China" (Heginbotham 2015, p. 259). In the years to come, it will be interesting to observe the cyber tactics used between the U.S. and China. The advent of cyberwarfare makes malicious activity against other nations more accessible. Although illustrated throughout this paper, some people disagree about the relevance of cyberwarfare on a global scale. According to the *Journal of Peace Research*, only a small percentage of international cyber issues escalate to be problematic; acts of cyberwarfare are rare, and "when they do happen, the impact tends to be minimal" (Valeriano and Maness 2014, p. 359). This stance would be contested by most national security experts in the U.S., because the impacts of cyberwarfare should hardly be described as "minimal."

CONCLUSION

The U.S. has vastly incorporated cyber policy and cyber strategies into post 9/11 national security efforts. The increase of computing machinery and internet usage in recent decades has led to an unprecedented convergence of technologies. Due to the increase in technology, there has been an accompanying increase in technological/cyber threats. Software vulnerabilities and exploitative viruses became apparent in the 1980s and malicious cyberattacks have occurred in and against the U.S. ever since. The terror attacks in New York City and Washington, D.C. on September 11th brought an increased awareness of online communication, surveillance methods, and terror prevention. Various members of Congress have introduced over 1,000 pieces of cyber-related legislation since 9/11, and over 90 of those pieces of legislation were signed by the president and became law (Figure 1 and Figure 2). These numbers reflect a substantial increase compared to pre-9/11 legislative statistics.

The Patriot Act has proven to be an extremely controversial law. However, it enables federal agencies to participate in surveillance activities that were previously prohibited; and these surveillance activities have offered excellent results, according to the FBI and NSA. Since the 9/11 attacks, over 50 attempted terror attacks have been thwarted according to data gathered by the Heritage Foundation (Figure 3). Many of these attacks were prevented through surveillance of online communication. In recent years, DoD and the Trump Administration have both established clear cyber strategies, chiefly consisting of affirmation for national security programs and encouraging an increased level of effective data sharing between agencies. Similarly, in recent years, the U.S. has used cyber tactics as an offensive strategy to gather intelligence and to prevent terror activities. From a global standpoint, cyber warfare and cyber-related activities have, to some extent, leveled the playing field between dominant and less-dominant state actors, because a cyberattack can be perpetuated by a small group of people, unlike a physical military attack. Due to the 53 thwarted terror attacks since 9/11, the U.S. has demonstrated the ability to adapt to the recent cyber and terror threats of this new technological era, which is crucial. As stated by the Director of National Intelligence, Daniel Coats, cyber vulnerabilities and potential cyberattacks against the U.S. are "at the top of the list of worldwide threats" (Garamone 2018, pp. 1).

The above discussion regarding post-9/11 cyber policy included the establishment of DHS, data-sharing legislation passed in Congress, Executive Orders regarding cybersecurity, and the Patriot Act. Although it took time to resolve initial issues with each of these policies, collectively, they have proven to be effective at preventing cybersecurity breaches and detecting online communications between terrorists. While it is important to consider areas for improvement, these policies should be used as a guide to influence future cyber policies in the U.S.

References

Arena, Kelli, and Kevin Bohn. 2004. “Al Qaeda Suspect Reveals Communication Strategy.” *CNN*. http://www.cnn.com/2004/US/08/03/terror.threat/index.html (December 5, 2018).

Armey, Richard. 2002. “H.R.5005 - 107th Congress (2001-2002): Homeland Security Act of 2002.” *Congress.gov*. https://www.congress.gov/bill/107th-congress/house-bill/5005 (February 25, 2019).

Bucci, Steven, James Carafano, and Jessica Zuckerman. 2013. “60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism.” *The Heritage Foundation*. https://www.heritage.org/terrorism/report/60-terrorist-plots-911-continued-lessons-domestic-counterterrorism (February 25, 2019).

Carper, Thomas R. 2014. “S.2519 - 113th Congress (2013-2014): National Cybersecurity Protection Act of 2014.” *Congress.gov*. https://www.congress.gov/bill/113th-congress/senate-bill/2519 (February 25, 2019).

Clinton, Larry. 2015. ”Best Practices for Operating Government-Industry Partnerships in Cyber Security." *Journal of Strategic Security.* vol. 8, no. 4: 53-68. https://www.jstor.org/stable/26465215.

Crosston, Matthew. 2014. “Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly.* vol. 6, no. 4: 100-18. http://www.jstor.org/stable/26270568.

Crowther, Glenn Alexander. 2017. ”The Cyber Domain." *The Cyber Defense Review.* vol. 2, no. 3: 63-78. http://www.jstor.org/stable/26267386.

“Cyberwarfare | Definition of Cyberwarfare in English by Oxford Dictionaries.” 2013. *Oxford English Dictionary*. https://en.oxforddictionaries.com/definition/cyberwarfare (February 25, 2019).

Department of Homeland Security. “National Cybersecurity & Communications Integration Center.” 2018. *Department of Homeland Security*. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (February 25, 2019).

Fruhlinger, Josh. 2017. “What Is Stuxnet, Who Created It and How Does It Work?” *CSO Online*. https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html (November 18, 2018).

Garamone, Jim. 2018. “Cyber Tops List of Threats to U.S., Director of National Intelligence.” *U.S. DEPARTMENT OF DEFENSE*. https://dod.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/ (February 25, 2019).

Goines, Timothy M. 2017. ”Overcoming the Cyber Weapons Paradox." *Strategic Studies Quarterly* vol. 11, no. 4: 86-111. http://www.jstor.org/stable/26271635.

Hathaway, Oona A., and Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-85. http://www.jstor.org/stable/23249823.

Heginbotham, Eric. 2015. *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996 - 2017*. Santa Monica, CA: RAND.

Kushner, David. 2013. “The Real Story of Stuxnet.” *IEEE Spectrum: Technology, Engineering, and Science News*. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (December 5, 2018).

Lange, Katie. 2018. “DOD's Cyber Strategy: 5 Things to Know.” *U.S. DEPARTMENT OF DEFENSE*. https://www.defense.gov/explore/story/Article/1648425/ (December 5, 2018).

Lieberman, Joseph I. 2012. “Text - S.2105 - 112th Congress (2011-2012): Cybersecurity Act of 2012.” *Congress.gov*. https://www.congress.gov/bill/112th-congress/senate-bill/2105/text (February 28, 2019).

McCaul, Michael T. 2018. “H.R.3359 - 115th Congress (2017-2018): Cybersecurity and Infrastructure Security Agency Act of 2018.” *Congress.gov*. https://www.congress.gov/bill/115th-congress/house-bill/3359 (December 5, 2018).

McGhee, James E. 2016. ”Liberating Cyber Offense." *Strategic Studies Quarterly.* vol. 10, no. 4: 46-63. http://www.jstor.org/stable/26271529.

Mobile Biometric Identification. 2010. *U.S. Code*. Title 46, Chapter 701. Subchapter I. Section 70123. Retrieved from http://uscode.house.gov (February 25, 2019).

Mueller, Robert. 2004. “USA PATRIOT Act.” *FBI*. https://archives.fbi.gov/archives/news/testimony/usa-patriot-act (March 1, 2019).

“National Commission on Terrorist Attacks Upon the United States: About the Commission.” 2004. *9/11 Commission*. http://govinfo.library.unt.edu/911/about/index.htm (February 25, 2019).

NATO. 2013. “The History of Cyber Attacks - a Timeline.” *North Atlantic Treaty Organization*. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm (December 5, 2018).

Newmeyer, Kevin P. 2012. “Who Should Lead U.S. Cybersecurity Efforts?" *PRISM.* vol. 3, no. 2: 115-26. https://www.jstor.org/stable/26469733.

Obama, Barack. 2013. “Executive Order -- Improving Critical Infrastructure Cybersecurity.” *National Archives and Records Administration*. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (February 28, 2019).

Oberstar, James L. 2010. “H.R.3619 - 111th Congress (2009-2010): Coast Guard Authorization Act of 2010.” *Congress.gov*. https://www.congress.gov/bill/111th-congress/house-bill/3619 (February 25, 2019).

Olenick, Doug. 2018. "Cyber Enemies of the United States." *SC Media*. https://www.scmagazine.com/home/security-news/in-depth/cyber-enemies-of-the-united-states/ (December 5, 2018).

Ratcliffe, John. 2017. "H.R.1616 - 115th Congress (2017-2018): Strengthening State and Local Cyber Crime Fighting Act of 2017." *Congress.gov*. https://www.congress.gov/bill/115th-congress/house-bill/1616 (December 5, 2018).

Savage, Charlie. 2018. "N.S.A. Triples Collection of Data From U.S. Phone Companies." *The New York Times*. https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html (December 5, 2018).

Schneider, Grant. 2018. "President Trump Unveils America's First Cybersecurity Strategy in 15 Years." *The White House*. https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/ (December 5, 2018).

Sensenbrenner, James. 2001. "H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001." *Congress.gov*. https://www.congress.gov/bill/107th-congress/house-bill/3162 (February 25, 2019).

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. *U.S. Code.* Title 6, Chapter 6. Subchapter 1. Section 1501. Retrieved from http://uscode.house.gov (February 25, 2019).

Tavani, Herman T. 2016. *ETHICS AND TECHNOLOGY: Controversies, Questions, and Strategies for Ethical Computing*. Hoboken, N.J.: Wiley.

Trump, Donald. 2017. "Statement by President Donald J. Trump on the Elevation of Cyber Command." *The White House*. https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/ (February 25, 2019).

Vaidya, Tavish. 2015. “The 20 Most Infamous Cyberattacks of the 21st Century (Part I).” *MIT Technology Review*. https://www.technologyreview.com/s/540786/the-20-most-infamous-cyberattacks-of-the-21st-century-part-i/ (December 5, 2018).

Valeriano, Brandon, and Ryan C Maness. 2014. ”The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11." *Journal of Peace Research.* vol. 51, no. 3: 347-60. http://www.jstor.org/stable/24557484.