CYBERSECURITY FINALLY TAKES CENTER STAGE IN THE U.S.

Kayla Morency*

I. Introduction

It is no secret that in the wake of globalization and the explosion of the Internet the world is more interconnected than ever.[1] The Internet provides access to content stored by governments, corporations, interest groups, institutions, and individuals to millions of users located across the globe on a daily basis.[2] It also provides users with

*J.D. Candidate, Suffolk University Law School, 2015; B.A. Roger Williams University, 2012.

[1] *See* Klaus W. Grewlich, GOVERNANCE IN 'CYBERSPACE': ACCESS AND PUBLIC INTEREST IN GLOBAL COMMUNICATIONS 21 (Kluwer Law International, 1999) (explaining the interconnectivity of communication networks); s*ee also* Gareth Grainger, *Freedom of Expression and Regulation of Information in Cyberspace: Issues concerning Potential International Cooperation Principles*, *in* THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 72-73 (UNESCO, 2000) (describing the development of the Internet in the 1960s and its transformation throughout the following decades). The Internet was created in the United States as a communications system for the military, but shortly thereafter, computer networks and the numbers of Internet users grew exponentially, due to its user-friendly accessibility at relatively low costs. *See id.* at 3 (outlining the history of cyberspace).

[2] *See* Grainger, *supra* note 1, at 9 (characterizing the Internet as a globalized mechanism for communication).

 ISSN 1536-7983.

the capabilities to create and disseminate their own material to other users regardless of their location.[3] It is essentially a "network of networks,"[4] where data is accumulated and participation is relatively inexpensive as compared with other media outlets.[5] As a result, the Internet is an integral part of modern-day life and it connects people "globally, regionally, and locally for business, research and education, and political and social interaction."[6]

In addition, "The United States…[is] among the world's largest cyber actors."[7] For example, computer networking systems are responsible for critical functions such as "managing and operating nuclear power plants, dams, the electric power grid, the air traffic control system, and the financial infrastructure."[8] Furthermore, computer networking systems play a fundamental role in the day-to-day operations of government, organizations, and companies by managing payroll, performing research and development, and conducting and tracking sales and the movement of goods.[9] However, due to the nation's reliance on computer networking systems and the interdependence of private citizens, sensitive data and information remains

[3] *See* Grainger, *supra* note 1, at 3 (describing the various functions of the Internet).
[4] *See* Matthew Burnstein, *A Global Network in a Compartmentalised Legal Environment*, 5 INTERNET: WHICH COURT DECIDES, WHICH LAW APPLIES? 23 (Katharina Boele-Woelki & Catherine Kessedjian eds., 1998).
[5] *See* Grainger, *supra* note 1, at 3 (describing the equipment needed for Internet access: a computer, a modem, and access to a telephone line).
[6] *See* Computer Sci. & Telecomm. Bd. Nat'l Research Council, CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 2 (National Academy Press 2002) [hereinafter CYBERSECURITY TODAY AND TOMORROW] (highlighting the critical functions of society which operate by computers and computer networking systems)*; see also* Grewlich, *supra* note 1, at 21 (characterizing Internet usage as an activity which crosses territorial boundaries).
[7] *See Report Says China Linked to Cyber-Attacks on Organizations in U.S., Other Countries*, BLOOMBERG BNA (Feb. 25, 2013), *archived at* http://perma.cc/6H2D-YSC5 (quoting White House spokeswoman, Caitlin Hayden).
[8] *See* CYBERSECURITY TODAY AND TOMORROW, *supra* note 6, at 2. Telecommunication systems, the Internet, computer systems, and the networks of information technology infrastructures are all factions within the umbrella of cyberspace and comprise the nation's critical infrastructure. *See* Marianne Stone, *Obama's Cybersecurity Plan*, SECURITY TECHNOLOGY POLICY PAPERS SERIES 1, 1 (Spring 2010) (defining the term cyberspace).
[9] *See* CYBERSECURITY TODAY AND TOMORROW, *supra* note 6, at 2 (highlighting the various functions that the Internet plays in modern society).

vulnerable to attack or exploitation; thus, the security of cyberspace remains a priority for the nation's public and private sectors.[10]

[10] *See* CYBERSECURITY TODAY AND TOMORROW, *supra* note 6, at 1-3; Grewlich, *supra* note 1, at 20-21 (summarizing the issue of cyber threats). "[O]ur nations, critical infrastructure, both physical and cyber, is the backbone of America's national security and economic prosperity." *See* Office of the Press Secretary, *Background Briefing on the Launch of Cybersecurity Framework*, THE WHITE HOUSE (Feb. 12, 2014), *archived at* http://perma.cc/AFS7-KFHE (explaining the significance of the nation's critical cyber infrastructure). In the 1997 Report of the President's Commission on Critical Infrastructures, *Critical Foundations: Protecting America's Infrastructures*, the report clearly recognized the significance of vital infrastructures and explained how these networks have become intertwined:

> These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructure to one another in a complex networks of interdependence. This linkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.

PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES, 9 (Oct. 1997), *archived at* http://perma.cc/BCD7-2WK8.

Due to societies' dependence on computer technology and the pivotal role it plays in national infrastructures, computers and networks have become an increasingly attractive and vulnerable target to outside nations during times of conflict. As a result, notions of traditional warfare are dissolving, and computer technology is being used as a "weapon for warfare." While a consensus among the international community regarding the appropriate vernacular remains to be resolved, the use of "cuber-attack" and "cyber warfare" have been used interchangeably often to reflect the mode of operation, which yields a deliberate interference, destruction, etc. of computer systems or networks. However, it is important to acknowledge that there are other ways to manipulate computer technology that do not involve the disturbance of "the normal functioning of a computer system; [but rather]…leverage[s] cyber capabilities to obtain confidential information otherwise inaccessible to the attacker." This Note will emphasize this latter form of manipulation, and it is most notably referred to as "cyber exploitation" or "cyber espionage." *See* Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1080-91 (2013) (highlighting the various components that may comprise a "cuber-attack").

In light of the September 11th tragedy, the United States' government and private industries reevaluated their focus on a variety of security measures, including cybersecurity.[11] As a result, several legislative efforts were made, and upon its own initiative, the private sector put more emphasis on developing software with the idea in mind that there is the potential for outsider intrusion at every level of its design.[12] In addition, the government allocated significant resources into researching and tracking cyber espionage and potential threats of cyber-terrorism.[13] Furthermore, private cybersecurity firms have risen, including Mandiant, a cybersecurity consulting firm located in Virginia, which has developed security software to help organizations with even the most aggressively secure networks to rapidly detect,

[11] *See* CYBERSECURITY TODAY AND TOMORROW, *supra* note 6, at 1 (acknowledging the September 11th attacks as the motivation to focus on cybersecurity research and development). The horrific terrorist attacks on September 11, 2001, demonstrated how quickly a substantial amount of lives and physical infrastructures lost and destroyed. Therefore, in the immediate aftermath, significant attention was drawn towards the nation's vulnerable infrastructures, including cyberspace, because a cuber-attack would compromise key information systems and computer networks, which would essentially disrupt or destroy the nation's vital institutions. As a result, the government honed in on various dimensions of cybersecurity in order to improve its ever-changing vulnerabilities. *See* CYBERSECURITY TODAY AND TOMORROW, *supra* note 6, 1-7 (explaining the implications of cyber-attacks); *see also infra* Part II.C (listing the legislative efforts taken in the political arena post the September 11th tragedy).

[12] *See* NAT'L RESEARCH COUNCIL AND NAT'L ACAD. OF ENG'G, THE NAT'L ACADS., TOWARDS A SAFER AND MORE SECURE CYBERSPACE 223-248 (Seymour E. Goodman & Herbert Lin eds., 2007) (detailing the legislative and administrative steps towards a more secure cyberspace). *See also id*. at 245 (discussing the realty of developing computer software among active adversaries).

[13] *See id*. at 266 (discussing the extent to which resources were allocated to research and development under the Cybersecurity Research and Development Act of 2002). In light of the "exponential increases in interconnectivity [that] have facilitated enhanced communications, economic growth, and the delivery of services critical to the public welfare, but have also increased the consequences of temporary or prolonged failure," Congress allocated substantial resources for "long term research funding" in order to "improve the vulnerability assessment and technological and systems solutions." *See also* Cyber Security Research and Development Act, Pub. L. No. 107-305, § 2, 116 Stat. 2367, (2002) (codified at 15 U.S.C.A. §§ 278h, 7401-7411) (highlighting Congressional findings leading up to the Act's passage).

analyze, and resolve security breaches.[14] However, Mandiant's investigative efforts came to the forefront, in February 2013, when it publicly released its controversial findings concerning their seven-year long investigation, which linked China to a major cyber espionage[15] campaign targeting several United States' business and industries.[16] Since the report's release, there has been widespread concern stemming from both the public and private sectors in determining what steps must be taken to reduce the United States' vulnerability to cyber-attacks.[17]

This note examines the current mechanisms in place for protecting computer-networking systems, reviews the findings of the Mandiant Report, and analyzes the highlights of President Obama's Official Framework for Improving Critical Infrastructure Cybersecurity as a comprehensive approach towards decreasing the United States' critical infrastructure vulnerabilities. In Part II, this note highlights an historical perspective of cybersecurity law in the United States, with particular emphasis on legislative efforts in the post-9/11 political arena. Part III acknowledges recent Congressional action

---

[14] *See* Sue Reisinger, *Cybersecurity Report Spotlights Risks to U.S. Business from China*, LAW JOURNAL NEWSLETTER, Mar. 1, 2013, at 7 (reporting the seven year project tracking Chinese cyber invasions); *see also Mandiant Platform*, MANDIANT (MAR. 31, 2014, 12:28 PM), *archived at* http://perma.cc/69VU-MHHW (explaining how Mandiant software equips security conscious organizations with the capabilities to identify threats present in networks so that advanced attacks can be stopped at the outset and compromised data restored).

[15] *See* CYBERSECURITY TODAY AND TOMORROW, *supra* note 6, at 3 (identifying potential targets and effects of cyber-attacks); Grewlich, *supra* note 1, at 21 (considering a variety of ways the Internet can be used maliciously by cyber criminals); Office of the Press Secretary, *supra* note 10 (highlighting the risks of cyber-attacks to America's national security and economic prosperity); Nguyen, *supra* note 10, at 1082 (examining the scope of cyber espionage in relation to international law violations).

[16] *See* William Wan & Ellen Nakashima, *Report Ties Cyberattacks on U.S. Computers to Chinese Military*, THE WASHINGTON POST (Feb. 19, 2013), *archived at* http://perma.cc/9R8M-RKUT (discussing the release of Mandiant's findings coupled with China's adamant albeit suspect denial of the accusations); *see also* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (2013), *archived at* http://perma.cc/J65E-UQLB (affirming China's involvement in a major cyber espionage campaign against the United States and other UN organizations).

[17] *See* Reisinger, *supra* note 14 (explaining the increased political pressure on the Obama administration and the expectation of increased dialogue among boardrooms).

and the recent developments leading up to the current state of affairs regarding cybersecurity policies, including a detailed summary of the key findings of the Mandiant Report. In Part IV, this note analyzes whether the Official Cybersecurity Framework is an adequate measure towards improving the nation's cybersecurity defenses. Furthermore, this note assesses whether Congress will have an important role in future cybersecurity policies. While legislation is important to create valuable infrastructure and allocate appropriate resources to research and development, this note argues that the Official Cybersecurity Framework is an excellent starting point towards improving the vulnerabilities of the nation's critical cybersecurity infrastructure, but it is only the beginning of long journey towards a comprehensive solution.

II. History

A. Cybercrime Defined

In light of the Information Age, crimes relating to computer networking systems are far beyond traditional, because these crimes transcend borders by inflicting harm "from anywhere and against any computer in the world."[18] Essentially, cybercrime refers to the unauthorized access to confidential computer networks and the unlawful meddling with systems, programs, and information.[19] However, cybercrimes take on a variety of forms.[20] For example, hacking into a computer system provides the user with access to read personal information, erase important data, or install a "digital time bomb," in which companies are forced to pay extortionists large sums of money.[21] Additionally, cybercriminals plant viruses that have the capacity to delete valuable material, spread other viruses, or disrupt the

[18] Marc D. Goodman & Susan W. Brenner, *Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J.L. & TECH. 3, 11 (2002) (discussing cybercrimes in which computers play only an incidental role).
[19] *See id.* (attempting to define cybercrime although there is no globally accepted definition).
[20] *See id.* at 12-16 (illustrating the broad range of activities that are considered cybercrimes). Although there are several subsets within the broader scheme of cybercrime, this note focuses on computer offenses.
[21] *See id.* at 12-13 (characterizing hackers as computer networking invaders).

company's productivity.[22] One of the most common forms of cybercrime is online fraud.[23] Cyber fraud can take the shape of counterfeiting, investment fraud, or stolen credit information.[24] Another major area of concern is cyberterrorism, which is defined as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which…[leads to] violence against noncombatant targets by subnational groups or clandestine agents."[25] Cyberterrorists possess the capabilities to cause major disruptions in banking, pharmaceuticals, air traffic control systems, or electronic power systems.[26] As a result, this final category has the potential to cause the most catastrophic destruction, including the death of thousands of innocent people.[27]

B. Calling Attention to Cybersecurity

Dating back to 1991, the United States' government acknowledged the nation's ever-increasing dependence on computers, which correlated to its ever-increasing vulnerabilities.[28] For example, in 1991, the National Research Council publicly announced:

> We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable to the effect[s] of poor de-

[22] *See id.* (describing the mode of cybercrime which involves disseminating viruses).
[23] *See id.* at 13 (acknowledging the correlation between increases in ecommerce and cyber fraud).
[24] *See* Goodman & Brenner, *supra* note 18, at 13-14 (recognizing the evolution of fraud in light of online transactions).
[25] *See* Goodman & Brenner, *supra* note 18 at 17 (attempting to define cyberterrorism).
[26] *See* Goodman & Brenner, *supra* note 18 at 17 (providing examples of industries vulnerable to cyberterrorist attacks).
[27] *See* Goodman & Brenner, *supra* note 18 (recognizing the devastating effects of cyberterrorism).
[28] *See* NAT'L RESEARCH COUNCIL AND NAT'L ACAD. OF ENG'G, *supra* note 12, at 223 (characterizing the future of cybersecurity in regards to its increased accessibility and usage).

> sign and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.[29]

This report was among the first to publicly announce that computer networking severely impairs the nation's cybersecurity.[30] In 1997, during the Clinton administration, the President's Commission on Critical Infrastructure Protection concluded that the exponential growth of a "computer literate population" guarantees that millions of users across the globe will posses the knowledge and capabilities to conduct a cyber attack, which reinforced the notion that cybersecurity should become a high priority concern at the top of the government's agenda.[31] Finally, during the George W. Bush administration, two

---

[29] *See* SYS. SEC. STUDY COMM., NAT'L RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 7 (1991). The National Research Council consists of members drawn from the National Academy of Sciences, the Nationals Academy of Engineering, and the Institute of Medicine. The council was created to bring together members of the science and technology communities in order to increase research and development to advise the federal government. *See id.* at R2 (illustrating the creation of the National Academies and the National Research Council).

[30] *See* NAT'L RESEARCH COUNCIL AND NAT'L ACAD. OF ENG'G, *supra* note 12, at 224 (summarizing the National Research Council's report). These presidential recognitions signified that cybersecurity is an imminent albeit growing threat to the nation's critical infrastructures. Despite these acknowledgements, political leaders made little advancement in the realm of cybersecurity initiatives, because there were little incentives within the political arena that required political leaders to make such efforts. Most notably, politicians were reluctant to impose increased costs to improve the nation's cybersecurity when the benefits of those costs would not be known to their constituents or even realized during their term in office. *See id.* at 226-227 (explaining the reasoning behind legislative inaction regarding cybersecurity in the past).

[31] *See* PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES (1997) (acknowledging the reality that resources used to engage in cyberwarfare are more readily available than that of chemical, biological, or nuclear weaponry). Since weaponry used in physical attacks are difficult to obtain by terrorists, the probability of cuber-attacks are dramatically increased due to the accessibility of computers. *See id.*

The *Critical Foundations* Report presents the conclusions made by President Clinton's Commission on Critical Infrastructures after a fifteen month evaluation of the

additional reports called attention to the threat of severe cyber attacks and acknowledged the vulnerability of critical infrastructures affecting the nation's overall economy and national security.[32] The overall goal of these reports was to engage the public in a dialogue in matters affecting their daily lives.[33]

C. Cybersecurity Policies in the United States

One of the earliest legislative efforts to protect citizens again cybercrime was the Computer Fraud and Abuse Act (CFAA).[34] The Act has been amended numerous times; however, as it reads today, the statute broadly prohibits (1) "knowingly caus[ing] the transmission of a program, information, code or command…and intentionally caus[ing] damage without authorization, to a protected computer;" (2) "intentionally access[ing] a protected computer without authorization, and…recklessly causes damages;" (3) "intentionally access[ing] a protected computer without authorization, and…causes damage and

nation's critical infrastructures, while focusing on their vulnerabilities. The Commission concluded that due to the "collective dependence on the information and communications infrastructure," the issue of critical cyber infrastructures should be viewed within the scope of national security. *See id.* at vii (prefacing the task President Clinton delegated to the Commission and stating the Commission's general conclusions).

[32] *See* NAT'L RESEARCH COUNCIL AND NAT'L ACAD. OF ENG'G, *supra* note 12, at 225-26 (emphasizing the dire consequences of potential cuber-attacks and the increasing sophistication of online users). *The National Strategy to Secure Cyberspace* acknowledged the threat of organized cyber-attacks and the availability of technical capabilities to wreak havoc on the nation's critical infrastructures. In addition, the *Cyber Security: A Crisis of Prioritization* recognized that the nation's information technology infrastructure is embedded into society; therefore, it logically follows that terrorists will inevitably take advantage of these opportunities to exploit the vulnerabilities of these technologies. Overall, these reports are just a few of many statements made during the past few decades that purport the notion that cybersecurity should be positioned at the forefront of national security concerns. *See id.* (summarizing two reports issued during George W. Bush's administration that encourage cybersecurity reform).

[33] *See* NAT'L RESEARCH COUNCIL AND NAT'L ACAD. OF ENG'G, *supra* note 12, at 225-26 (alerting the citizens of the United States to the growing problem of cuber-attacks).

[34] *See* Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2006) (protecting citizens against cybercrime).

loss."[35] However, according to the provision of the statute, the definition of "protected computer" is narrow and largely limited to computers used by the federal government or financial institutions.[36]

In the immediate aftermath of the September 11th attacks, President George W. Bush issued Executive Order 13231 on October 16, 2001.[37] The order called attention to the technological revolution responsible for the new ways in which business was transacted, government was operated, and national defense policies were accomplished.[38] As a result, the order demanded the protection of these information systems to prevent any interference with the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.[39] Furthermore, the order created the National Infrastructure Advisory Council (NIAC), which later became absorbed by the Department of Homeland Security.[40] The NIAC was responsible for making recommendations about the security of the nation's critical economic infrastructures and the U.S. national security.[41]

---

[35] *See id.* § 1030 (a)(5)(A-C) (defining several punishable actions).
[36] *See* Brian B. Kelly, *Investigating in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. REV.1663, 1683 (2012) (explaining the pitfalls of the CFAA).
[37] *See* Exec. Order No. 13, 231, 66 Fed. Reg. 53,063 (Oct. 16, 2001) (issuing a governmental policy to protect against the disruption of information systems); *see also* RITA TEHAN, CONG. RESEARCH SERV., R42507, CYBERSECURITY: AUTHORITATIVE REPORTS AND Resources 21 (2013) (defining executive order as "official documents through which the President of the United States manages the operations of the federal government").
[38] *See* Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2011) (stating the policy supporting President Bush's executive order).
[39] *See id.* (explaining provisions of President Bush's executive order).
[40] *See* NAT'L RESEARCH COUNCIL AND NAT'L ACAD. OF ENG'G, *supra* note 12, at 267 (establishing the NIAC in order to improve the nation's cybersecurity). Under Executive Order 13286 issued on February 28, 2003, the NIAC became a part of the Department of Homeland Security, by amending the existing Executive Order 13231. The amendment of the executive order transferred certain functions, including the NIAC, to the Secretary of Homeland Security to streamline processes and increase efficiency in resolving the national security issue. The terms of the amendment required the NIAC to report and advise the Secretary of Homeland Security on the security of critical cyber infrastructures. *See* Exec. Order No. 13,286, 66 Fed. Reg. 10,619 (Feb. 28, 2003) (amending Executive Order 13231).
[41] *See id.* (explaining the duties and responsibilities of the newly created council).

The Federal Information Security Management Act of 2002[42] (FISMA) was passed, which provided a mechanism for improving the management and oversight for information security programs of federal agencies.[43] It also required the National Institute of Standards and Technology (NIST) to establish mandatory cybersecurity procedures for all federal agencies engaging in information sharing.[44] This initiative included minimum guidelines for adequate information security of all agency operations but did not apply to national security systems.[45] However, the Act was largely criticized for being ineffective in supervising cybersecurity practices and outcomes.[46]

In 2002, Congress passed the Cybersecurity Research and Development Act[47], which called for significant investments in research and development for computer networking security.[48] The Act aimed to assess the vulnerabilities of computer networking systems and to identify solutions to the growing cybersecurity problems.[49] Moreover, it called for an increase in the number of cybersecurity professionals and the improvement of data sharing between the government, industries, and academia.[50] It also delegated these responsi-

[42] *See* 44 U.S.C. § 3541 (2006) (establishing a comprehensive framework for effective information security controls used by federal governmental operations).
[43] *See id.* (describing the statutory provisions of FISMA).
[44] *See* Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, § 303(a)(3) (2002) (recognizing the need for uniform security procedures when engaging in information sharing). The NIST is a part of the U.S. Department of Commerce and acts as the nation's oldest physical science laboratory, and it provides measurement science and standards that encourages innovation in all areas of technology including global communication networks. *See About NIST*, NIST, *archived at* http://perma.cc/WR5A-RTRG (describing the functions of the NIST).
[45] *See* Federal Information Security Management Act § 303 (explaining the applicability of the FISMA).
[46] *See* Kelly, *supra* note 36, at 1684 (acknowledging that several high-ranking officials criticized the FISMA for failing to adequately secure governmental computer systems).
[47] *See* Cybersecurity Research and Development Act, Pub. L. No. 107-305, 116 Stat. 2367 (2002) (allocating substantial resources to cybersecurity research and development).
[48] *See id.* at § 5 (authorizing appropriations to establish new higher education programs for computer and network security).
[49] *See id.* at § 22 (establishing a program to support research to improve the security of computer systems).
[50] *See id.* at §§ 2(5), 22 (encouraging more professionals to study cybersecurity).

bilities to a variety of governmental agencies, including the National Science Foundation, the National Institute of Standards and Technology, and the newly created Department of Homeland Security.[51]

The National Plan for Research and Development in Support of Critical Infrastructure Protection[52] was issued in April 2005 and focused on several key components, such as: "(1) creat[ing] a baseline, including the identification of existing research and technology development efforts within federal agencies and (2) [articulating] a vision that takes into account the future needs and identifies research gaps based on known threats."[53] In addition, this plan identified nine categories, which incorporated both cyber and physical security concerns: (1) detection and sensor systems; (2) protection and prevention; (3) entry and access portals; (4) insider threats; (5) analysis and decision-support systems; (6) response, recovery, and reconstitution; (7) new and emerging threats and vulnerabilities; (8) advanced infrastructures and systems design; (9) and human and social issues.[54] Overall, the plan prioritized these areas of research and development into long and short-term goals.[55] However, it exemplified a comprehensive outlook and plan for the future of cybersecurity research and

[51] *See id.*at § 13 (providing examples of agencies responsible for carrying out the goals of the Cybersecurity Research and Development Act of 2002).
[52] *See National Plan for Research and Development in Support of Critical Infrastructure Protection*, THE EXECUTIVE OFFICE OF THE PRESIDENT AND THE DEPARTMENT OF HOMELAND SECURITY, vii (2004) *archived at* http://perma.cc/3H8Q-MYNC (addressing research and development issues not covered in the 2005 Interim National Infrastructure Protection Plan). The National Infrastructure Protection Plan was issued in 2006 and established national goals and priorities for critical infrastructure and key resources. *See National Infrastructure Protection Plan*, THE DEPARTMENT OF HOMELAND SECURITY, i (2006) *archived at* http://perma.cc/CPW6-9SZW (specifying the "key initiatives, milestones, and metrics required to achieve the Nation's [critical infrastructure and key resources] protection mission").
[53] *National Plan for Research and Development in Support of Critical Infrastructure Protection*, *supra* note 52, at xii.
[54] *See National Plan for Research and Development in Support of Critical Infrastructure Protection*, *supra* note 52, at 15-16 (detailing the nine themes of research and development in which cyber security and physical security overlap).
[55] *See National Plan for Research and Development in Support of Critical Infrastructure Protection*, *supra* note 52, at 15 (describing the organization and prioritization of the nine areas of research and development).

development while aligning the efforts of stakeholders to manage evolving threats and discover gaps of vulnerability.[56]

In June 2006, the Department of Homeland Security released the National Infrastructure Protection Plan,[57] which provided for "an integrated, comprehensive approach to addressing physical, cyber, and human threats and vulnerabilities to address the full range of risks to the Nation."[58] In the event that critical infrastructures were violated, the plan provided directions to identify and prioritize assets and implement protective measures in each infrastructure sector.[59] Furthermore, the plan delegated responsibilities to the stakeholders to ensure effective implementation.[60] Overall, the plan called for a collaborative effort between all levels of government and the private sector.[61]

III. Facts

"The cybersecurity threat is real, imminent, and growing in severity."[62] However, despite this acknowledgement, there have been few successful attempts to combat this reality.[63] Unfortunately, solutions to the growing cybersecurity problem involve a game of cost-risk analysis, where the risk amounts to small-losses in the present versus *potentially* substantial losses in the future.[64] Moreover, while substantial costs are incurred at the outset, in order to be proac-

---

[56] *See National Plan for Research and Development in Support of Critical Infrastructure Protection*, *supra* note 52, at xii (providing for an all-inclusive approach when tackling cybersecurity research and development).
[57] *See National Infrastructure Protection Plan*, *supra* note 52 (explaining the significance of the NIPP).
[58] TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 268.
[59] *See National Infrastructure Protection Plan*, *supra* note 52, at 31-35 (explaining the organized procedures to address imminent cybersecurity threats).
[60] *See National Infrastructure Protection Plan*, *supra* note 52, at 23 (describing the various actors involved in the implementation process, including stakeholders, who are the individuals affected in the event of a breach).
[61] *See National Infrastructure Protection Plan*, *supra* note 52, at iii (stating the objectives of the NIPP).
[62] TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 223.
[63] *See* TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12,at 223-28 (explaining the characteristics of the persisting political arena in light of cybersecurity threats and potential solutions).
[64] *See* TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 223-28 (highlighting the implications presented to legislators by engaging in cybersecurity policy discussions).

tive, benefits are typically not realized within a politician's term in office.[65] Since benefits are not realized until a later point in time, few politicians are willing to bear this burden of advocating for cybersecurity solutions.[66] Individuals prefer to run the risk of cybersecurity attacks, because they believe that the probability of the occurrence of a cyber-attack is extremely low.[67] However, there are extremely significant consequences at stake.[68] As a result, these conditions, which continue to persist, prevent the establishment of a comprehensive solution to the problem, and it continues to worsen over time.[69]

A. Congress's Role in Cybersecurity Policies

Despite growing concern, there have been very few successful legislative provisions enacted since 2002.[70] In 2002, the Cyber Security Research and Development Act was enacted, which allocated substantial resources and funding for long-term research and development in the cybersecurity industry, but since this time, no major

---

[65] *See* TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 227 (explaining the reluctance of politicians to allocate substantial resources to cybersecurity solutions when benefits may not be realized in the foreseeable future).

[66] *See* TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 227 (highlighting the problems political leaders face when attempting to resolve cybersecurity issues).

[67] *See* TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 227 (explaining that the uncertainty of solutions coupled with the high initial costs create a disincentive to political action); *see also* Ellen Nakashima, *U.S. said to be Target of Massive Cyber-espionage Campaign* (Feb. 10, 2013), *archived at* http://perma.cc/U8LW-KNGH (quoting a former government official stating, "[t]he problem with foreign cyber-espionage is not that it is an existential threat, but that it is invisible, and invisibility promotes inaction").

[68] *See* TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 227 (comparing an historically low probability of cyber invasions to the detrimental consequences that may result).

[69] *See* TOWARDS A SAFER AND MORE SECURE CYBERSPACE, *supra* note 12, at 227 (determining that the failures of cybersecurity measures are due in part to a lack of political activism).

[70] *See* TEHAN, *supra* note 37, at 1 (highlighting the lack of cybersecurity legislation); *see also* John Grant, *Will There Be Cybersecurity Legislation?*, 4 J. NAT'L SECURITY L. & POL'Y 103, 11 (2010) (explaining Congressional action is more swift when encouraged by external factors, such as the slew of legislation passed after the September 11, 2001, terrorist attacks).

legislative action has been particularly successful.[71] Although cyber threats have been persistent throughout the last decade, these incidents have not produced a lasting impact on the general public, which discourages Congress to enact cybersecurity policies.[72] For example, the Securely Protect Yourself Against Cyber Trespass Act[73] attempted to prohibit unfair or deceptive practices in connection with (1) gaining access or unsolicited control of a protector computer; (2) modifying computer settings; (3) collecting personally identifiable information; (4) removing, disabling, or rendering a computer's anti-spyware or anti-virus technology inoperative; etc.; however, several versions of the Act failed to reach fruition and died either in the House or Senate.[74] The Cybersecurity Acts of 2010[75] and 2012[76] both shared a similar fate.[77] The Cybersecurity Act of 2010 was designed to (1) facilitate the free flow of commerce within the United States and between its global partners through secure cyber communication systems; (2) provide for increases in the development of cybersecurity studies among industry specialists; and (3) improve cybersecurity defenses.[78] Unfortunately, the Act was introduced in the Senate on April 1, 2009 but died in Committee as reported on March

---

[71] *See* Cyber Security Research and Development Act, *supra* note 13, at 2367-68 (explaining provisions of the Act); *see also* Grant, *supra* note 70, at 111 (acknowledging little societal pressure to enact cybersecurity legislation).

[72] *See* Grant, *supra* note 70, at 111 (identifying the lack of public concern and awareness for cybersecurity threats).

[73] *See* Securely Protect Yourself Against Cyber Trespass Act, H.R. 964, 110th Cong. § 2 (2007) (prohibiting any person from gaining unauthorized access to a protected computer).

[74] *See H.R. 964 (110th): Securely Protect Yourself Against Cyber Trespass Act*, GOVTRACK.US, a*rchived at* http://perma.cc/LE7S-R6K5 (summarizing the bill and providing its status).

[75] *See* Cybersecurity Act of 2010, S. 773, 111th Cong. (2010) (directing the President to develop a comprehensive national cybersecurity strategy).

[76] *See* Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012) (ordering the Department of Homeland Security to work with other federal agencies and private industry organizations to conduct a cybersecurity infrastructure risk assessment and develop cybersecurity defenses).

[77] *See S. 773 (111th): Cybersecurity Act of 2010*, GOVTRACK.US, *archived at* http://perma.cc/TJS6-T9DD (reporting the status of the Cybersecurity Act of 2010); *see also S. 2105 (112th): Cybersecurity Act of 2012*, GOVTRACK.US, *archived at* http://perma.cc/WJ99-7MKX (reporting the status of the Cybersecurity Act of 2012).

[78] *See* Cybersecurity Act of 2010, *supra* note 75 (stating the provisions of the Act).

24, 2010.[79] The Cybersecurity Act of 2012 intended to "enhance the resiliency of the cyber and communications infrastructure;" however, the Act similarly died in committee.[80] On July 24, 2013, the Cybersecurity Act of 2013[81] was introduced in the Senate.[82] Essentially, the Act provided for an ongoing partnership between the public and private sectors to improve cybersecurity and strengthen cybersecurity research and development while increasing public awareness.[83] The Act is currently being debated in committee; however, it is estimated that the Act only has a thirty-six percent chance of passage.[84]

Despite Congress's failure to present a united front and make meaningful improvements towards a comprehensive cybersecurity policy, one successful policy has been enacted, which is Congress's support for National Cyber Security Awareness Month.[85] The National Cyber Security Awareness Month is celebrated every October and was created under the Department of Homeland Security and the National Cyber Security Alliance.[86] Since its creation almost ten years ago, the goal has been to raise public awareness about the critical cybersecurity issues facing the public and private sectors in the United States.[87] Congress has publicly supported the month through resolutions, and President Obama has even issued Presidential Proclamations declaring October as the National Cyber Security Awareness Month.[88] Even though there have been few bipartisan cybersecurity legislation enacted, Congressional support for National Cybersecurity Awareness Month draws necessary attention to the

---

[79] *See S. 773 (111th)*, *supra* note 77 (reporting the bill status).
[80] *See S. 2105 (112th)*, *supra* note 77 (reporting the bill status).
[81] *See* Cybersecurity Act of 2013, S. 1353, 113th Cong. (2013) (attempting to enhance public awareness and strengthen the cybersecurity collaboration between the public and private sectors).
[82] *See id.* (providing the factual background of the bill's introduction).
[83] *See id*. (stating the purpose of the Cybersecurity Act of 2013).
[84] *See S. 1353: Cybersecurity Act of 2013*, GOVTRACK.US, *archived at* http://perma.cc/E7QM-7MK7 (reporting the status of the bill).
[85] *See* S. Res. 306, 112th Cong. (2011) (enacted) (agreeing to support the goals of ideals of National Cyber Security Awareness Month).
[86] *See About National Cyber Security Awareness Month*, STAYSAFEONLINE.ORG, archived *at* http://perma.cc/KW4E-UX8R (providing the history of National Cyber Security Awareness Month).
[87] *See id.* (explaining the goal of the National Cybersecurity Awareness Month).
[88] *See id.* (acknowledging that the President has publicly supported National Cyber Security Awareness Month).

growing issue, which will hopefully translate into increased political pressure on Congress to develop more comprehensive cybersecurity policies.[89]

B. A Necessary Wake-up Call

Despite challenges that legislators face in the political arena, major developments have recently stirred up widespread concern over cybersecurity measures.[90] For example, shortly after taking the presidential oath, President Obama pledged a commitment to securing the nation's cybersecurity network.[91] Moreover, upon taking office, President Obama ordered the Cyberspace Policy Review,[92] which was a sixty-day compressive review of the current United States policies and procedures regarding cybersecurity.[93] The review was lengthy and spurred a great deal of conversation on Capitol Hill; however, the report did not generate as much public awareness on the crucial issue as government officials intended.[94] About a year later, President Obama released a statement regarding his Comprehensive

---

[89] *See* Grant, *supra* note 70, at 111 (stating "there has been no sizeable public clamor for action on cybersecurity").

[90] *See* Reisinger, *supra* note 14 (reporting the project of tracking Chinese cyber invasions); s*ee also* Amber Corrin, *White House Unveils Cybersecurity Framework*, FCW (Feb. 12, 2014), *archived at* http://perma.cc/CG82-Y9XW (announcing a new cybersecurity framework addressing critical infrastructure protection).

[91] *See* Kelly, *supra* note 36, at 1664 (explaining the importance of cybersecurity in relation to the President's political agenda). During that same speech, President Obama even acknowledged the he was a victim of a cyber-attack during his 2008 Presidential campaign, which largely incorporated social media and the Internet. *See id.* In particular, the computer networking system was hacked, and the hackers were able to access a variety of campaign files, ranging from travel plans to policy position papers. *See id*. at n.2 (underscoring the idea that almost all computer systems are vulnerable to cuber-attack under the current state of cybersecurity policies).

[92] *See Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, THE WHITE HOUSE, at iii (Jan. 2009), *archived at* http://perma.cc/UK9V-3647 (reporting the findings of a 60 day comprehensive investigation of the nation's current state of cybersecurity polices and protections).

[93] *See id.* at iii (describing the executive summary of the review).

[94] *See* Kelly, *supra* note 36, at 1687 (suggesting that there needs to be an increase in public awareness in order for cybsersecurity policies to be enacted and implemented).

National Cybersecurity Initiative.[95] In the initiative, President Obama acknowledged cybersecurity as the "most serious economic and national security challenge" facing the nation.[96] In order to help implement Obama's Cyberspace Policy Review,[97] the initiative would incorporate and build upon the Comprehensive National Cybersecurity Initiative (CNCI)[98] established by President George W. Bush.[99] President Obama used former President Bush's efforts to develop and update a more comprehensive national cybersecurity strategy.[100] This effort included twelve stated objectives working towards three primary goals: (1) "to establish a front line of defense against today's immediate threats"; (2) "to defend against the full spectrum of threats"; and (3) "to strengthen the future cybersecurity environment."[101]

In February 2013, The National Intelligence Estimate, which represents the consensus among the U.S. intelligence community, identified China as the most prolific actor "aggressively seeking to

---

[95] *See The Comprehensive National Cybersecurity Initiative*, THE WHITE HOUSE (Mar. 2010), *archived at* http:// perma.cc/47HE-MC3H (describing how cybersecurity is a serious threat to the nation's economic prosperity and national security).
[96] *See id.* (declaring a compelling need to act against cybersecurity attacks).
[97] *See Cyberspace Policy Review*, *supra* note 92 at iii (outlining the scope and strategy of the cyberspace policy).
[98] *See* John Rollins & Anna C. Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, CONGRESSIONAL RESEARCH SERVICE (Mar. 2009), *archived at* http://perma.cc/KG9K-HQHH (stating that President George W. Bush established the CNCI in 2008 in order to make the nation more secure from cyber threats).
[99] See Rollins & Henning, *supra* note 98, at 1 (establishing the "policy, strategy, and guidelines to secure federal systems").
[100] *See The Comprehensive National Cybersecurity Initiative*, *supra* note 95 (describing President Obama's intention to utilize and build upon existing cybersecurity procedures to prevent any reinvention of the wheel).
[101] *See The Comprehensive National Cybersecurity Initiative*, *supra* note 95 (outlining the goals of the comprehensive national cybersecurity initiative). Some initiatives involve consolidating the management of the federal enterprise network into a single enterprise with trusted internet connections; deploying an intrusion detection system across the federal enterprise to identify unauthorized users that gain access to the networks; coordinating and redirecting research and development efforts to eliminate redundancy in federally funded cybersecurity research; enhancing situational awareness among the federal information security offices; expanding cyber education to increase the number of cybersecurity experts within the federal government or private sector; developing deterrence strategies and programs for cyber defenses; etc. *Id.* (explaining the twelve initiatives in detail).

penetrate the computer systems of American businesses and institutions to gain access to data that could be used for economic gain."[102] The document highlighted the broad spectrum of sectors that have been vulnerable to attack within the last five years, including finance, aerospace, automotive, information technology, and finance.[103] Although the report failed to calculate the financial impact of China's efforts, experts in the field have estimated it to be tens of billions of dollars.[104] China firmly rejected the cyber espionage allegations and refuted the notion that the government engages in hacking activities; however, since the 1980's the U.S. has been aware that Chinese intelligence services have attempted to recruit its own citizens to steal trade secrets and gain insider access to U.S. corporate networks.[105] Therefore, claims of cyber espionage seem credible.

Within a few days of the release of the National Intelligence Estimate, Mandiant, a computer security firm located in Alexandria, Virginia, affirmatively linked the Chinese government to a major cyber espionage campaign since at least 2006.[106] After the news spread of this tangible proof, many reporters, politicians, and business institutions referred to the report as a "wakeup" call, highlighting the immediate need for cybersecurity legislation or a comprehensive approach to minimize these threats.[107] In addition, Mandiant's Vice President, Grady Summers, hoped that "Th[e] report…[would] elevate the dialogue to the boardroom and to the general counsel of-

---

[102] *See* Nakashima, *supra* note 67 (identifying China as the most aggressive country trying to penetrate computer systems in America).
[103] *See* Nakashima, *supra* note 67 (describing the wide range of sectors that have been susceptible to cyber invasion).
[104] *See* Nakashima, *supra* note 67 (explaining the financial impact of China's cyber espionage attacks).
[105] *See* Nakashima, *supra* note 67 (recognizing that the Chinese government has attempted to acquiesce sensitive corporate information in the United States within the last few decades).
[106] *See* Alexei Alexis, *Report Links China to 'Cyber Espionage' Campaign Against U.S., Other Countries*, BLOOMBERG BNA, 99 Fed. Cont. Rep. 223, Feb. 26, 2013 (exposing the details of Mandiant's findings which suggest the Chinese government sponsored a cyber espionage campaign against several organizations, particularly located in the United States).
[107] *See id*. (advocating for a streamlined approach to oppose cuber-attacks and protect American industries).

fice."[108] Overall, the very public release of the Mandiant Report has placed significant pressure on the Obama administration and has made cybersecurity a more transparent and relatable problem for the American people.[109] Although efforts to eliminate cybersecurity threats have been somewhat ineffective up until now, the release of the Mandiant Report has spurred widespread concern from both the public and private sectors, which may provide enough motivation in order to effectively resolve or reduce these cybersecurity threats.[110]

C. *Mandiant's Findings*[111]

[108] *See* Reisinger, *supra* note 14 (discussing the desired effect the Mandiant report will have on cybersecurity).
[109] *See* Reisinger, *supra* note 14 (recognizing the devastating impact of cyber crimes and encouraging companies to report suspected breaches to the appropriate law enforcement outlet).
[110] *See* Mandiant, *supra* note 16, at 2 (describing the success of China's state sponsored espionage efforts).
[111] *See* Mandiant, *supra* note 16, at 2 (providing the factual background of Mandiant's investigation). Mandiant is a computer security firm located in Alexandria,

1. Identity of APT1

After Mandiant's seven year long investigation, it determined that the Communist Party of China directed the Chinese People's Liberation Army (PLA) to commit cyber espionage and data theft against organizations located around the world.[112] Furthermore, Mandiant concluded that the PLA cyber command is located within the PLA's 3rd Department of the General Staff Department (GSD), which is largely responsible for the operational guidance of defense information systems.[113] The GSD 3rd Department is further broken

---

Virginia. *See also Contact Us*, MANDIANT, *archived at* http://perma.cc/L7U3-VAGY (displaying the location of Mandiant company headquarters). It has investigated the security breaches of hundreds of organizations located around the globe. Since 2004, most of the security breaches that were discovered were characterized as advanced threat actors and referred to as the "Advanced Persistent Threat" (APT). Within the last few years, evidence has surfaced, which suggests that the groups engaging in these cybersecurity breaches are located in China and are known to the Chinese government. The Mandiant Report focuses on the most prolific group, which Mandiant refers to as APT1, and the report explains that the group is most likely a government-sponsored organization. Although, APT1 is only one out of over twenty APT groups located in China, Mandiant has tracked APT1 and its cyber intrusions from 2006 to 2013, and it concluded that there have been almost one hundred fifty victims over the seven-year period, in which sensitive information has been stolen. Based on observations of APT1's tactics and procedures, Mandiant determined that there are actual individuals who are operating from behind APT1's keyboards and engaging in this cyber espionage campaign. *See also* Mandiant, *supra* note 16, at 2-3 (providing the factual background of Mandiant's investigation).

[112] *See* Mandiant, *supra* note 16, at 7 (concluding that APT1 was given direct governmental assistance and was thus a state sponsored venture). The Chinese Communist Party (CCP) was formed in 1921 by Mao Zedong and took control of China at the end of World War II in 1945, by defeating the Nationalist Army. By 1949, the Communist People's Republic of China (PRC) was formed and led by Mao. The CCP is a hierarchical system with great power vested in a selected leader. Among the several wings within the CCP is the military wing, known as the People's Liberation Army (PLA). *See Modern China: The Promise and Challenge of an Emerging Superpower*, WORLD SAVVY MONITOR (Apr. 5, 2014), *archived at* http://perma.cc/VZW5-XFJX (summarizing the history of the CCP).

[113] *See* Mandiant, *supra* note 16, at 7 (comparing the GSD to the US Joint Chief of Staff). The PLA, which is the military wing of the CCP, is broken down into several subparts. For example, the General Staff Department (GSD) is one of the most superior departments in the PLA, and it is comparable to the United States Joint Chief of Staff. The GSD "establishes doctrine and provides operational guidance

down to into twelve bureaus and three research institutes, including the 2nd Bureau.[114] Through the use of public records and acknowledgements, Mandiant determined that the APT1 operation is situated within the 2nd Bureau and was given the Military Unit Cover Designator 61398 (Unit 61398).[115] In addition, Mandiant's research supports the conclusion that Unit 61398 functions as the GSD's 3rd Department's primary operations system and is responsible for targeting any predominately English-speaking organization by investigating into its political, economic, and military-related intelligence.[116] Finally, Mandiant contends that Unit 61398 received direct governmental support for its cyber espionage operations by utilizing China's state-owned enterprises.[117]

According to the size of Unit 61398's infrastructure and China's public disclosures, Mandiant estimated that APT1 has hundreds, if not thousands, of employees, and is located in a twelve-story building with 130,663 square feet of office space in Gaoquiaozhen, in the Pudong New Area of Shanghai.[118] Mandiant also determined that the

for the PLA." Within the GSD are more subcategories, including the 3rd Department, which focus on intelligence, foreign language proficiency, and defense information systems. It is presumed to be a large unit with an estimated personnel of 130,000 and consists of 12 bureaus and 3 research institutes. Throughout its seven-year long observation, Mandiant determined that the APT1 cyber command is located within the 2nd Bureau of the GSD 3rd Department. *See* Mandiant, *supra* note 16, at 7-8 (emphasizing the sheer magnitude of the organizational structure).

[114] *See* Mandiant, *supra* note 16, at 7-8 (explaining the hierarchy of the PLA and GSD).

[115] *See* Mandiant, *supra* note 16, at 9 (acknowledging public references which implicate Unit 61398 as the entity responsible for computer network operations). Unit 61398 is an example of a Chinese military unit (MUCD). MUCDs are given a five-digit code, which ensures the anonymity of the unit and its functionality. *See* Mandiant, *supra* note 16, at 9 (explaining that Unit 61398 is a Chinese military unit). It is important to acknowledge Mandiant concluded "APT1" is the Chinese military unit 61398; therefore, based on this premise, the two terms will be used interchangeably for the purposes of this note.

[116] *See* Mandiant, *supra* note 16, at 9 (finding Unit 61398's computer network operations expand beyond the United States and Canada).

[117] *See* Mandiant, *supra* note 16, at 7-8 (recognizing state-owned enterprises that directly supported 61398's activities). In China, the military and government are subordinate to the political party known as the Communist Party of China. Therefore, it must follow that any cyber espionage activity was approved or directed by the leaders of the Communist Party of China. *See id.* at 7.

[118] *See* Mandiant, *supra* note 16, at 11-12 (providing statistics recorded during Mandiant's investigation).

building was large enough to hold an estimated two thousand employees.[119] There are additional buildings, which comprise an assortment of support units including a kindergarten, an outpatient clinic, and guesthouses.[120] These facilities underscore the proposition that Unit 61398 is a high-level position in the PLA hierarchy.[121]

During its investigation, Mandiant found a Chinese memorandum, which acknowledged governmental support of Unit 61398 and confirmed the unit's placement in the 2nd Bureau of the GSD 3rd Department.[122] In a letter sent from the state-owned enterprise, China Telecom, executives revealed a plan to "co-build" with Unit 61398 and use China Telecom inventory in the construction of fiber optic communications lines.[123] In addition, China Telecom revealed that it possessed an abundance of inventory "to satisfy the military's request."[124] Furthermore, China Telecom laid out the method of rental payment for the 2nd Bureau and its intent to provide Unit 61398 with an agreement for its signature and subsequent implementation.[125] Overall, the letter supported Mandiant's above conclusions that not only was the Chinese government aware of Unit 61398's cyber operation, but it provided the Unit with direct support in the form of fiber optic communication infrastructure.[126]

---

[119] *See* Mandiant, *supra* note 16, at 11-12 (emphasizing the level of infrastructure held at the cyber command center).

[120] *See* Mandiant, *supra* note 16, at 16 (acknowledging the services and amenities that accompany the cyber command center).

[121] *See* Mandiant, *supra* note 16, at 16. (inferring the importance of Unit 61398's activities to the national defense intelligence based on its significant resources).

[122] *See* Mandiant, *supra* note 16, at 16 (referencing a letter sent from China Telecom executives).

[123] *See* Mandiant, *supra* note 16, at 16 (providing the details of the memorandum which emphasizes the relationship between China Telecom and Unit 61398). China Telecom is a telecommunications provider and "the world's largest wireline telecommunications, CDMA mobile network, and broadband Internet services provider." It provides Internet access and information services in the PRC. *See* CHINA TELECOM (Apr. 5, 2014), *archived at* http://perma.cc/GQ6-BXHT (describing the company's purpose).

[124] *See* Mandiant, *supra* note 16, at 18 (highlighting China Telecom's correspondence with the military regarding their inventory of fiber-optic cables).

[125] *See* Mandiant, *supra* note 16, at 18 (detailing the terms of an apparent agreement between China Telecom and Unit 61398).

[126] *See* Mandiant, *supra* note 16, at 16-18 (translating China Telecom's internal memorandum that acknowledges the existence of and agrees to support Unit 61398).

2. APT1's Focus

Mandiant's investigation discovered APT1's cyber exploitations of a variety of industries since 2006, but first, it is important to acknowledge the geographic locations of these organizations and the industries targeted by APT1's efforts.[127] The evidence obtained throughout the study revealed that APT1's cyber-attacks primarily targeted victims in English speaking countries.[128] For example, one hundred fifteen victims were located in the United States and seven in Canada and the United Kingdom.[129] Moreover, seventeen of the remaining nineteen victims all used English as the primary language for their operating systems.[130] These alarming statistics help explain why English-language proficiency is required for almost all Unit 61398 personnel.[131]

Due to the broad range of information gathered, it was clear to Mandiant that APT1's "mission [was] extremely broad."[132] For example, Mandiant categorized the scope of information stolen from the 141 victim organizations into twenty major industries, including: information technology, transportation, financial services, navigation, legal services, energy, food and agriculture, engineering services, aerospace, etc.[133] However, the report explains that the range of industries APT1 targeted may be even broader than Mandiant's evidence suggests, because the figure only represents a fraction of

---

[127] *See* Mandiant, *supra* note 16, at 21 (detailing Mandiant's observations of the scope and location of organizations targeted by APT1).
[128] *See* Mandiant, *supra* note 16, at 21 (explaining APT1's generally targeted cyber actors).
[129] *See* Mandiant, *supra* note 16, at 21 (emphasizing that the United States was the nation targeted in significantly greater proportions than that of other English speaking countries).
[130] *See* Mandiant, *supra* note 16, at 21 (acknowledging that the remaining two non-English speaking victims were outliers in the course of APT1's regular activities).
[131] *See* Mandiant, *supra* note 16, at 21 (drawing comparisons between Mandiant's investigation of APT1 and the PLA's Unit 61398).
[132] *See* Mandiant, *supra* note 16, at 22 (contending that APT1's ability to steal from a wide range of industries simultaneously gives them a broad target base).
[133] *See* Mandiant, *supra* note 16, at 23 (illustrating the computer networking compromises by industry sector).

APT1's victims that were directly confirmed by the cybersecurity firm.[134]

By examining the types of industries that were compromised, Mandiant attempted to decipher China's strategic purpose for engaging in this cyber espionage campaign.[135] The firm concluded that some of the industries that were targeted significantly more than others were at least four out of the seven strategic emerging industries contained within China's 12th Five Year Plan, which was an initiative by the Chinese government to boost its economy by encouraging domestic consumerism, increasing the quality of manufacturing, and providing governmental support for these "strategic emerging industries."[136] However, it is evident from Mandiant's findings that the goals of APT1's cyber espionage campaign closely paralleled China's economic goals that were proclaimed in March 2011, which further suggests that APT1 is Unit 61398, and its efforts were a state-sponsored cyber attack.[137]

Mandiant's evidence confirmed that APT1 stole hundreds of terabytes of sensitive data from the computer networking systems of more than 141 organizations located across the globe.[138] Once APT1

---

[134] *See* Mandiant, *supra* note 16, at 22 (acknowledging that the figure only represents a fraction of *confirmed* victims).

[135] *See* Mandiant, *supra* note 16, at 24 (explaining Mandiant's analytical approach to APT1's cyber espionage campaign).

[136] *See* Joseph Casey & Katherine Koleski, *Backgrounder: China's 12th Five-Year Plan*, U.S.-CHINA ECONOMIC & SECURITY REVIEW COMMISSION 1 (Apr. 5, 2014), *archived at* http://perma.cc/4RST-QMQR (summarizing China's efforts to restructure the economy through new industrial policies). The 12th Five Year Plan emphasizes seven strategic industries as "the drivers for China's future economic development," which includes: (1) clean energy technology; (2) next-generation information technology; (3) biotechnology; (4); high-end equipment manufacturing; (5) alternative energy; (6) new materials; and (7) clean energy vehicles. *See id*. at 8.

[137] *See id*. at 1 (stating the date China's 12th Five Year Plan was released); *see also* Mandiant, *supra* note 16, at 24 (surmising that the Chinese government may have a played an active role in APT1's cyber espionage campaign based on similarities between the industries exploited and China's governmental objectives).

[138] *See* Mandiant, *supra* note 16, at 25 (emphasizing the extent of APT1's cyber exploitations). A terabyte is about one trillion bytes. Essentially, a single terabyte could hold about three hundred hours of good quality video or one thousand copies of the Encyclopedia Britannica. *See also Megabytes, Gigabytes, Terabytes What are They?* WHAT'S A BYTE, *archived at* http://perma.cc/3246-9VWK (explaining the significance of a terabyte).

gained access to a victim's computer network, the Unit accessed the network periodically over a course of months or years and stole significant amounts of data including "technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from the victim organizations' leadership."[139] Moreover, Mandiant concluded that on average APT1 maintained access to a victim's network for 356 days (about one year), and the longest recorded period, in which it maintained continuous access was at least 1,764 days (four years and ten months).[140]

Although Mandiant lacks direct evidence regarding the ways in which China uses the stolen information, Mandiant discovered a remarkable connection between a company that was directly involved in wholesale transactions with the People's Republic of China and whose computer networking system was compromised.[141] Mandiant also reported that APT1 stole sensitive data from several organizations practically at the same time.[142] For example, in January 2011, APT1 acquired access to seventeen new computer networks located among ten different industries.[143] However, considering that access to a victim's network persisted on average for about a year, Mandiant concluded that these newly acquired computer networks were ac-

---

[139] *See* Mandiant, *supra* note 16, at 20 (outlining the victims' valuable information technology targeted by APT1).

[140] *See* Mandiant, *supra* note 16, at 21 (listing statistics regarding APT1's ability to sustain access to their victims networks).

[141] *See* Mandiant, *supra* note 16, at 25 (providing a case study of a company whose computer networking system was compromised and inferring how the information stolen may have provided a substantial advantage to China). For more than two and a half years, APT1 stole an unknown amount of information from the victim company and repeatedly accessed several executives' email accounts, including the Chief Executive Officer and the General Counsel. Coincidentally, China managed to negotiate a significant decrease in its deal with the company regarding one of its major commodities. This surprising deal was even reported by major media outlets. Although there is no direct evidence in support of Mandiant's conclusion, this incident may suggest the ways in which China capitalizes on the stolen information resulting from its cyber espionage activities. *See* Mandiant, *supra* note 16, at 25 (explaining potential implications resulting from China's cyber exploits).

[142] *See* Mandiant, *supra* note 16, at 22 (describing the broad range of APT1's cyber espionage activities).

[143] *See* Mandiant, *supra* note 16, at 22-23 (listing examples of victims in newly acquired industries: scientific research and consulting, construction and manufacturing, aerospace, healthcare, and education).

cessed while simultaneously maintaining access to existing networks.[144] Since the Unit did not target a few specific industries throughout the course of the investigation but rather consistently obtained a vast amount of data from a plethora of industries, Mandiant concluded that not only "APT1's mission is extremely broad," but also the scope and nature of its activities imply that the Unit has significant resources and technical support.[145]

D. Official Cybersecurity Framework

In follow up to the growing cybersecurity threat, President Obama released Executive Order 13636[146], on February 12, 2013, which called for improvements in the critical infrastructure of cybersecurity standards and the development of a cybersecurity framework.[147] Additionally, the order called for cybersecurity information sharing between the public and private sectors by disseminating unclassified reports to the private sector in order to better protect these targeted entities.[148] However, President Obama's executive order came to fruition on February 12, 2014, with the release of the Official Framework for Improving Critical Infrastructure Cybersecurity.[149] The framework was the product of immense collaboration between

---

[144] *See* Mandiant, *supra* note 16, at 22 (explaining the process in which APT1 acquired access to new and existing victims' networks).

[145] *See* Mandiant, *supra* note 16, at 22 (inferring from the sheer magnitude and simultaneous nature of the Unit's cuber-attacks that the group must have substantial personnel and other resources at its disposal).

[146] *See* Improving Critical Infrastructure Cybersecurity, 78 FR 11739 (Feb. 12, 2013) (committing to improve cybersecurity infrastructure).

[147] *See id*. at 11740-41 (ordering the implementation of new policies and procedures to address the growing threat to the nation's cybersecurity). Some cybersecurity experts and economists have estimated that the cost of cyber espionage to the United States might range from 0.1% to 0.5% of the nation's gross domestic product, or in other words $25 billion to $100 billion dollars. *See* Nakashima, *supra* note 67 (linking China to a cyber-espionage campaign against the U.S. and explaining the substantial implications it may have on the nation's economy).

[148] *See* Improving Critical Infrastructure Cybersecurity, *supra* note 146, at 11739 (maximizing the utility of cybersecurity information with the private sector).

[149] See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 1 (Feb. 12, 2014), *archived at* http://perma.cc/Q7LU-EY8F [hereinafter *Framework for Improving Critical Infrastructure Cybersecurity*] (publishing the first version of a comprehensive model approach for assessing and resolving cybersecurity risk management issues).

the public and private sectors and took about a year to formulate.[150] Essentially, the framework aimed to provide a cost-effective approach to address and manage cybersecurity risks without placing additional and mandatory regulations on businesses.[151] The language within the framework emphasizes that it is a voluntary process, but it encourages businesses and organizations, all of whom have unique risks with varied threats, vulnerabilities, and tolerances to risks, to assess their own needs and implement the best practices wherever needed in order to reduce and manage cybersecurity risks in an effective way.[152]

"The Framework is a risk-based approach to managing cybersecurity risk;" therefore, it is dependent upon the business, organization, or agency to assess their cybersecurity vulnerabilities on an in-

[150] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 1 (describing that the framework resulted from external, expert assistance rather than being developed by government officials alone). It is important to acknowledge that on October 22, 2013, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) released a Preliminary Cybersecurity Framework; therefore, it was the precursor to the Official Cybersecurity Framework. The purpose of the public release of the Preliminary Framework was to encourage feedback during the NIST's forty-five day public comment period before the Official Framework was set to release in February 2014. The Preliminary Framework was the result of President Obama's Executive Order that the NIST work with stakeholders in the private sector to develop a voluntary framework to reduce the nation's cybersecurity risks (both publicly and privately). As a result, the NIST hosted a series of workshops during 2013, in which the NIST collaborated with more than 3,000 organizations and individuals, in order to assess cybersecurity industry standards and best practices to provide businesses, consumers, and governmental agencies insight on improving critical informational technology infrastructure. *See NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments*, NIST, *archived at* http://perma.cc/63KH-PJNM (discussing the backdrop behind the Preliminary Cybersecurity Framework's release); *see also* Office of the Press Secretary, *supra* note 10 (acknowledging that the Official Framework was the product of input from thousands of participants across the country after drafts were publicly released to encourage feedback and increase participation in its development).

[151] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 1 (recognizing that regulatory schemes are not an effective mechanism for managing cybersecurity threats).

[152] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 2 (emphasizing that the framework is not mandatory but rather voluntary in order to encourage skeptics or those with more experience to join the cybersecurity conversation and use the framework as a model for improvements).

dividualized basis.[153] The framework is broken into three components: (1) Framework Core; (2) Framework Implementation Tiers; and (3) Framework Profile.[154] Each component "reinforces the connection between business drivers and cybersecurity activities."[155] As a result, a successful risk-management analysis relies on an assessment of each component fully, because it aims to provide a comprehensive mechanism for identifying and resolving cybersecurity threats.[156]

The first division, Framework Core, is further broken down into five functions: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover.[157] These five functions serve as the strategic "lifecycle" that an organization's management should follow when assessing cybersecurity risk.[158] By charting these functions, as the Framework suggests, the organization is more apt to understanding

---

[153] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 4 (describing the framework as a risk based approach). Each business entity has unique cybersecurity risks that must be assessed and monitored via a fluid framework. *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 3.

[154] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 4-5 (identifying the structure of the framework).

[155] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 4.

[156] *See* Wyatt Kash, *Why Business Can't Ignore US Cybersecurity Framework: Industry Leaders and President Obama Call the Framework a First Step in Creating a Cybersecurity Playbook for 16 US Critical Infrastructure Sectors*, INFORMATIONWEEK (Feb. 14, 2014), *archived at* http://perma.cc/6ZT8-WWRE (acknowledging that the framework provides the questions that CEO's should be asking their companies regarding its cybersecurity practices).

[157] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 4 (listing the five categories within the Framework Core).

[158] *See supra* note 149 and accompanying text (stating that this framework is the first comprehensive approach to assessing cybersecurity risks); *see also Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 4-5 (describing the five functions of the Framework Core). The first category focuses on the cyber activities being conducted and the desired outcome the organization is seeking. In order to progress towards that goal, the cyber actor should look towards industry standards, best practices, cybersecurity guidelines, etc. that would encourage communication among the executive level down through the implementation phase at the operations level. *See Official Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 4-5 (summarizing the first division of the framework).

the impact of investing in cybersecurity risk-management.[159] It is also important to note that the five core functions are intended to be performed concurrently and continuously to maximize productivity and "form an operational culture that addresses the dynamic cybersecurity risk."[160]

The second division, Framework Implementation Tiers, is further broken down into four tiers (Tier 1-4), which should reflect the current state of the organization's management of cybersecurity risks and how the organization's risk management can improve and towards a higher tier.[161] To determine which Tier an organization fits into, the organization shall take into account: (1) the organization's current risk management practices; (2) the threat environment; (3) legal and regulatory requirements; (4) business objectives; and (5) institutional constraints.[162] Organizations are encouraged to strive towards a greater numbered Tier, so long as it is cost effective and would reduce cybersecurity risk.[163]

The final division, Framework Profile, indicates the overall outcome that a business is seeking to achieve.[164] In order to select a

---

[159] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 7 (providing examples that prove investment in planning and exercise yield increases in response and recovery thus reducing the impact of the delivery of services).

[160] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 8 (commenting on the fluidity of the framework).

[161] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 5 (explaining that the tiers reflect the degree an organization's cybersecurity risk management practices correlate to the framework's model approach).

[162] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 9 (explaining that an organization's success under the framework is not determinative of the Tier level but rather the organization's Target Profile under the third component). It is evident that this component is a completely individualized assessment of how the organization views its current cybersecurity risks as it relates to its mechanisms that resolve said risks. *See id.*

[163] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 9 (explaining that the goal of the second component is not solely to reach a higher level tier).

[164] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 5 (explaining that the significance of the profiles is to conduct self-assessments and foster in-depth communications within the organization or between organizations). The final division breaks down profiles into "Current Profile" and "Target Profile" in order for the organization to articulate and visualize where the business currently stands and where it would like to be at the end of its

Framework Profile, the business must identify its opportunities to improve and choose which standards, guidelines, and best practices will best address those needs.[165] The Current Profile represents the cybersecurity outcomes that the organization may achieve, but the Target Profile represents the outcomes the organization needs to achieve to reach its cybersecurity risk management goals.[166]

The Framework is not intended to replace existing cybersecurity practices, rather it is designed to supplement existing business operations systems and be incorporated as a systematic process for identifying, assessing, and managing cybersecurity risks.[167] In order to implement the Framework, the executive level should communicate its cybersecurity objectives to the individuals involved at the business-processing level.[168] Moreover, it is important for executives to discuss the available resources at the outset in order to maximize cost efficient resolutions.[169] The business-processing group should then contact the individuals responsible for operations systems in order to collaborate and develop the organization's cybersecurity Profile.[170] After implementation is underway, the operations systems should conduct an impact assessment and report their findings to the

efforts. In this stage, only the organization alone can determine its cybersecurity risks and ability to manage; therefore, it is imperative that the business invests appropriate resources in determining where it aligns and where it diverges from industry practices and cybersecurity policies. *See id.*

[165] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 5 (identifying the hopeful outcome after an organization completes the three step process); *see also infra* Part IV.A (discussing the criticisms of the official cybersecurity framework).

[166] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 11 (explaining that an organization must compare the two profiles in order to meet its cybersecurity objectives).

[167] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 13 (signifying the importance of the framework and explaining its intended use).

[168] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 12 (describing the process for implementing the framework).

[169] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 12 (acknowledging what resources are available will help the organization prioritize its needs and develop its Target Profile).

[170] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 12 (depicting the stages involved for implementation).

business-processors.[171] Then the business-processors will inform the executives of the organization's overall risk management process.[172] These steps help illustrate how an organization can create or revise its cybersecurity program, and it is meant to be a recurring process considering that cybersecurity threats are constantly evolving thus altering an organization's problem areas.[173]

IV. Analysis

A. Successes and Pitfalls of the Official Cybersecurity Framework

Industry leaders were quick to assess President Obama's Official Cybersecurity Framework.[174] Most consider the framework a major turning point in addressing the nation's cybersecurity vulnerabilities.[175] For example, the framework was responsible for establishing a foundation so that both the public and private sectors can work together towards achieving a common goal.[176] Moreover, the framework provided a "new shared vocabulary about cybersecurity that will allow CEO's, boards of directors and policymakers – not just here in the U.S., but around the world—to set baselines and chart the course for improvement and actually make those improvements."[177]

---

[171] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 12 (illustrating the cyclical nature of the process and explaining that it should run concurrently and continuously).
[172] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 12 (signifying the importance of transparency within the process).
[173] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 13 (urging organizations to conduct the process simultaneously and continuously).
[174] *See* Kash, *supra* note 156 (discussing initial reactions regarding the release of the official cybersecurity framework).
[175] *See* Office of the Press Secretary, *supra* note 10 (acknowledging that the Official Cybersecurity Framework is the first major step towards protecting the nation's critical infrastructures regardless of past failed legislative attempts to develop effective and efficient policies).
[176] *See* Office of the Press Secretary, *supra* note 10 (emphasizing that the cybersecurity issue cannot be resolved by either the government or the private sector alone but rather the two must work together towards a common goal).
[177] *See* Office of the Press Secretary, *supra* note 10 (quoting a Senior Administration Official as he summarized the development of the official cybersecurity framework).

A positive outcome that stems from the Official Cybersecurity Framework is its approach to partnerships and collaboration.[178] Seeing as though cyber threats are constantly evolving, the conversation needs to be a continuous one, where members from all sectors of the industry, such as large or small businesses and firms, are encouraged to participate.[179] The framework itself was the product of a massive collaborative effort.[180] Seeing as though government officials did not have all of the answers, the creation of the framework welcomed thousands of participants from across the country.[181] Moreover, drafts of the framework, including the Preliminary Cybersecurity Framework, were released on the NIST's website and feedback was welcomed.[182] Considering that the Official Cybersecurity Framework was the product of tremendous input from an array of experts,

[178] *See* Office of the Press Secretary, *supra* note 10 (noting that the official cybersecurity framework is the product of a yearlong collaboration among industry experts and government officials). President Obama's emphasis on the collaboration and partnership with industry specialists is an attempt to boost the framework's credibility among the private sector, which will hopefully garner support and motivate additional organizations within the private sector to join the conversation. *See* Office of the Press Secretary, *supra* note 10 (repeating a Senior Administration Official as he provided guidance to generate support for the official cybersecurity framework).

[179] *See* Office of the Press Secretary, *supra* note 10 (recognizing that no single group of people has all of the answers to address the cybersecurity issues therefore increased participation is needed in the future for an even more successful framework). Another reason that the private sector is encouraged to participate is due to the fact that the private sector has more resources, and if the framework is voluntary rather than mandatory, there is more incentive for shareholders to join the discussion. *See* Office of the Press Secretary, *supra* note 10 (identifying reasons that support private sector involvement in further developing the official cybersecurity framework).

[180] *See* Office of the Press Secretary, *supra* note 10 (referencing the five workshops held across the country and the drafted frameworks that were released to the public for comments and feedback); *see also NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments*, *supra* note 150 (describing the "tremendous amount of industry input" that was devoted to creating the Preliminary Cybersecurity Framework).

[181] *See* Office of the Press Secretary, *supra* note 10 (stating that there were five workshops held around country in which thousands of industry experts attended in order to develop the official cybersecurity framework).

[182] *See NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments*, *supra* note 150 (referring to the Preliminary Cybersecurity Framework that was released in October 2013 for a forty-five day public comment period).

the framework has a significant amount of credibility.[183] The recommendations did not stem from Washington politicians, but rather industry experts who have personally combatted cyber-attacks.[184]

Another key success of the Official Cybersecurity Framework is that it provides a consensus among private and public industry leaders regarding what is required for a comprehensive cybersecurity program.[185] As a result, the framework acts as a useful tool for organizations to achieve a competitive advantage over other businesses by lowering the cybersecurity threat to its consumers.[186] Moreover, the framework is the first "useful set of federally endorsed practices for private sector security" and is not "just another set of NIST guidelines."[187] Rather, it is anticipated that the Official Cybersecurity Framework will become the "de facto standard for private sector cybersecurity in the eyes of U.S. lawyers and regulators."[188] As a result, many industry leaders consider the framework a precedent for defining common cybersecurity standards.[189]

Another important characteristic of the framework is its flexibility.[190] The framework calls cybersecurity risk management to the attention of the stakeholders to determine what their cybersecurity objectives are in light of their available resources.[191] It is up to the company to

---

[183] *See* Office of the Press Secretary, *supra* note 10 (explaining that industry experts have more experience and no personal incentives to gain from their voluntary participation in the developmental process).

[184] *See* Kash, *supra* note 156 (reiterating that the framework did not result from the government wielding its regulatory authority but rather delegating responsibility to agencies, including the NIST, who was responsible for collecting and incorporating industry feedback).

[185] *See* Office of the Press Secretary, *supra* note 10 (explaining the accomplishments of the official framework).

[186] *See* Office of the Press Secretary, *supra* note 10 (explaining that implementing the program will make a business more attractive to consumers due to a dramatic decrease in cybersecurity threats).

[187] Kash, *supra* note 156.

[188] Kash, *supra* note 156 (resulting from congressional inaction regarding this issue).

[189] *See* Kash, *supra* note 156 (acknowledging the lack of standardized vocabulary and the lack of a comprehensive approach until the Official Cybersecurity Framework was released).

[190] *See* Office of the Press Secretary, *supra* note 10 (highlighting the successes of the framework).

[191] *See* Office of the Press Secretary, *supra* note 10 (describing the implementation process set forth in the official framework).

determine where it currently stands in terms of threats and protections as well as the company's vision regarding where it would like to be situated in the future.[192] As a result, it lays the basic groundwork for an organization to assess its current cybersecurity risks and protections under its cybersecurity operations.[193]

The framework also encourages a wide range of stakeholders to participate in future conversations, because the framework is voluntary rather than a government mandated regulation.[194] Since "voluntary standards are a tradition in the U.S.," they are more apt to be met with meaningful discussion.[195] Moreover, considering that the private sector has more resources at its disposal, incorporating private sector volunteers ensures that the companies will be more likely to abide by and implement the framework while making the necessary improvements for future progress.[196]

Finally, another accomplishment of the framework is that it serves as notice to Congress that the executive can make substantial efforts towards alleviating issues of national importance.[197] As discussed earlier, Congress has been unable to successfully collaborate and develop a comprehensive approach towards resolving the nation's cybersecurity vulnerabilities.[198] However, the Official Cybersecurity Framework is proof that the executive is sufficiently capable

---

[192] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 1 (explaining that the framework is a voluntary program that is intentionally broad so that a wide range of organizations can implement the program based on its current needs).

[193] *See* Office of the Press Secretary, *supra* note 10 (acknowledging that the program is individualized rather than a one-size fits all approach).

[194] *See* Office of the Press Secretary, *supra* note 10 (inferring that stakeholders would be more willing to join the cybersecurity conversation if the government is encouraging their opinions rather than mandating standardized regulations).

[195] Office of the Press Secretary, *supra* note 10.

[196] *See* Office of the Press Secretary, *supra* note 10 (recognizing that improving cybersecurity policies is a lengthy and costly process; therefore, private resources are necessary to ensure successful developments).

[197] *See* Kash, *supra* note 156 (acknowledging congressional inaction does not hinder progress at the executive level when it concerns threats to national security and economic prosperity).

[198] *See supra* Part III.A (discussing congressional cybersecurity policies).

of tackling this grave threat to the nation's security without Congress's assistance.[199]

One major critique of the framework is that it is too broad to accomplish any substantial protections.[200] As a result, some critics consider the framework nothing "more than a compilation of established industry security practices."[201] In addition, other critics emphasize that the framework lacks a metric for measuring success and fails to incentivize the implementation of its policies and practices.[202]

However, these criticisms are unfounded, because although the private sector advances through its competitiveness, organizations will be afforded more room for innovation since there is no need to reinvent the wheel and reproduce or develop cybersecurity protections that have already been discovered.[203] Moreover, the framework is intentionally broad, because no two businesses are alike and an organization's needs are constantly evolving.[204] As a result, it is the organization's responsibility to determine its own strengths, weaknesses, and projected goals.[205] While the framework is not intended to resolve all of the problems relating to cybersecurity, it is a major step in the right direction, and it fosters valuable channels of commu-

---

[199] *See* Kash, *supra* note 156 (reiterating that despite Congress' failures the executive branch has made significant progress regarding cybersecurity policies).
[200] *See* Office of the Press Secretary, *supra* note 10 (highlighting a common criticism of the framework).
[201] Kash, *supra* note 156.
[202] *See* Corrin, *supra* note 90 (stating three failures of the official cybersecurity framework and explaining that without proper incentives organizations will abandon the government's objectives).
[203] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 2 (explaining that a one-sized fits all approach would not address the various needs of all sectors and industries affected by cyber threats). The best way for these organizations to enhance their prosperity and productivity is to take advantage of information sharing, in order to keep progress and innovation moving forward, rather than expending significant resources on cybersecurity protection and risk management without the assistance and experience of outside organizations. *See id.* at 2.
[204] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 6 (signifying that the framework is intentionally broad).
[205] *See Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 149, at 4-5 (illustrating the organization's responsibility in implementing the framework's three components).

nication for future development and protection of the nation's critical infrastructures.[206]

B. Congressional Capacity to Enact Cybersecurity Legislation

As discussed earlier, there have been few successful attempts to combat the cybersecurity dangers that threaten the nation.[207] There are institutional weaknesses within the legislative branch that hinder its ability to effectively address the nation's cybersecurity vulnerabilities.[208] For example, corporate constituents wield immense power over the legislative agenda.[209] Furthermore, other significant issues, such as: climate change and the regulation of financial institutions, compete with cybersecurity for congressional attention.[210] Considering the time constraints within Congress and the fact that cybersecurity is a complex issue, any potential for a successful piece of legislation must take the form of a "relatively non-controversial bill that will attract few amendments and consume little precious floor time."[211]

Another factor that discourages congressional involvement in cybersecurity policies is the fact that there is little political pressure stemming from constituents.[212] Unlike the September 11th terrorist attacks, the public has been unaware of any significant and prolonged threat to cybersecurity.[213] As a result, there is "no sizable public clamor for action on cybersecurity."[214] However, in light of the re-

---

[206] *See* Office of the Press Secretary, *supra* note 10 (recognizing that the official cybersecurity framework does not solve all of the nation's critical infrastructures problems but rather provides a comprehensive mechanism that will hopefully lead towards a resolution).

[207] *See supra* Part III.A (highlighting congressional inaction).

[208] *See* Grant, *supra* note 70, at 110 (explaining the inherent weaknesses of the legislative branch).

[209] *See* Grant, *supra* note 70, at 110 (suggesting that legislators are not quick to veer away from the opinions of their corporate constituents).

[210] *See* Grant, *supra* note 70, at 110 (explaining that cybersecurity is only one of many significant issues presented to the legislature).

[211] *See* Grant, *supra* note 70, at 111-12 (suggesting that the technical nature of cybersecurity briefings may surpass the educational limits of members within Congress).

[212] *See* Grant, *supra* note 70, at 111 (recognizing cybersecurity is not at the forefront of public awareness).

[213] *See* Grant, *supra* note 70, at 111 (acknowledging that the sheer magnitude of the 9/11 attacks warranted significant public attention; however, cybersecurity threats have simply not been given a similar level of awareness).

[214] Grant, *supra* note 70, at 111.

cent developments, including the Mandiant Report and the release of the Official Cybersecurity Framework, there is potential for increased pressure on Congress, but due to its current institutional constraints, it does not appear that any meaningful legislative policies will be enacted in the near future.[215]

V. Conclusion

"We must come to think of cybersecurity in the same way that our country has come to think of increased traditional counterterrorism: as associated with real and existing threats," because the Internet is a public good that an inter-connected America depends on each and every day.[216] Furthermore, every governmental agency and almost every business entity has an online presence that is vulnerable to cyber exploitation. Therefore, President Obama appropriately characterized cyber threats as one of the gravest national security dangers in the United States.[217] It must follow then that the nation recognizes cybersecurity as a present danger, because it consists of measures that are personal, corporate, federal, and international. As a result, it is a function that is dispersed among society. Therefore, it is not solely the responsibility of the government, the private sector, or private citizens, but rather a shared responsibility to alleviate these threats. With the assistance of the Official Cybersecurity Framework, there is great potential for significant breakthroughs in the protection of the nation's cybersecurity and economic prosperity.

[215] *See supra* Part III (highlighting the recent developments calling attention to the nation's cybersecurity threats).
[216] Kelly, *supra* note 36, at 1711.
[217] *See* Kash, *supra* note 156 (summarizing President Obama's commitment to improving the nation's cybersecurity policies).