# FROM BOMBS AND BULLETS TO BOTNETS AND BYTES: CYBER WAR AND THE NEED FOR A FEDERAL CYBERSECURITY AGENCY

DANIELLE WARNER*



* Class of 2012, University of Southern California Gould School of Law; B.A. International Relations 2007, Tufts University; M.A. Government, Diplomacy and Conflict Studies 2009, The Interdisciplinary Center, Herzliya, Israel. Many thanks to Professor Edwin Smith for his insight throughout the development of this Note, Shannon Raj for her patience and guidance throughout the note process, and the members of the *Southern California Law Review* for their diligent editing. I also owe sincere gratitude to Jon, my parents and the rest of the Dubey-Warner clan for their unwavering love and support.

*The most likely way for the world to be destroyed, most experts agree, is by accident. That's where we come in; we're computer professionals. We cause accidents.*

—Nathaniel Borenstein[1]

## I. INTRODUCTION

In September 2010, Iranian engineers detected that a sophisticated computer worm, known as Stuxnet, had infected and damaged industrial sites across Iran, including its uranium enrichment site, Natanz.[2] In just a few days, a sophisticated computer code was able to accomplish what six years of United Nations Security Council resolutions could not. Not a single missile was launched, nor any tanks deployed, yet the computer worm effectively set back the Islamic Republic's nuclear program by two years and destroyed roughly one-fifth of its nuclear centrifuges.[3] The worm itself included two major components. One was designed to send Iran's nuclear centrifuges spinning out of control, damaging them. The other component seemed right out of the movies; "the computer program . . . secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart."[4]

1. Bornstein is one of the original designers of the Multipurpose Internet Mail Extensions ("MIME") protocol for formatting email.

2. David E. Sanger, *Iran Fights Malware Attacking Computers*, N.Y. TIMES, Sept. 26, 2010, at A4.

3. William J. Broad, John Markoff & David E. Sanger, *Israel Tests Called Crucial In Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; Yaakov Katz, *Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years*, JERUSALEM POST, Dec. 15, 2010, *available at* http://www.jpost.com/Iranianthreat/News/Article.Aspx?Id=199475.

4. Broad, Markoff & Sanger, *supra* note 3.

Stuxnet, to date, is the most sophisticated cyber weapon ever deployed.[5] It acted as a "collective digital Sputnik moment,"[6] bringing to light the important cybersecurity challenges the world faces. What makes cyber attacks so destructive is their ability to travel through the Internet and attack the structures it rests upon. Governments, industrial and financial companies, research institutions, and billions of citizens worldwide heavily populate these global networks. In fact, much of public and private life depends on functioning telecommunications and information-technology infrastructures. Thus, what we deemed to be one of the greatest successes of the twenty-first century, a global communication infrastructure, has now become our biggest vulnerability.

While Stuxnet is a more recent large-scale cyber attack to receive media attention, thousands of smaller cyber attacks happen every day, all over the world, on various government and private websites and networks. In 2007, there were almost 44,000 reported incidents of malicious cyber activity.[7] Everyday, millions of automatic scans operating from foreign sources search American computers and networks for vulnerabilities.

Many large U.S. companies have experienced firsthand the effects of these cyber attacks. In the last two years, Google,[8] MasterCard, Visa, PayPal,[9] and Citigroup[10] all experienced cyber attacks sufficient in size to obstruct their normal operations or obtain critical confidential information. In March 2011, the drafting of this Note was even (coincidentally) hindered by a cyber attack on the University of Southern California Law School's network. The virus, which is rumored to have originated in Hong Kong, shut down all of the school's networks, preventing access to email and data for several days.

American institutions, however, are not the only targets of cyber attacks. Critical infrastructures, including electrical grids, satellites, oil and

5. Pascal Mallet, *Stuxnet Worm Brings Cyber Warfare Out of Virtual World*, AFP, Oct. 1, 2010, http://www.google.com/hostednews/afp/article/ALeqM5hWP5Ga_K2k4oOosfMz39JFifrDaQ?docId=CNG.0c3a53ff7267f11501a5b3dbd9567dbf.2d1.

6. René Obermann, Op-Ed, Digital Sputnik Moment, INT'L HERALD TRIB., Feb. 27, 2011, at 8, *available at* http://www.nytimes.com/2011/02/28/opinion/28iht-edoberman28.html.

7. *Threats to the Information Highway: Cyber Warfare, Cyber Terrorism and Cyber Crime*, LIPMAN REP., Oct. 15, 2010, at 1, http://www.guardsmark.com/Files/Computer_Security/TLR_Oct_10.pdf [hereinafter LIPMAN REPORT].

8. *See* Andrew Jacobs & Miguel Helft, *Google May End Venture in China over Censorship*, N.Y. TIMES, Jan.13, 2010, at A1; John Markoff, *Cyberattack On Google Said to Hit Password System*, N.Y. TIMES, Apr. 20, 2010, at A1.

9. *See* Aaron Smith, *MasterCard, Visa Targeted in Apparent Cyberattack*, CNN MONEY, Dec. 8, 2010, http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/index.htm.

10. *See* Andrew Khouri, *Citigroup Hack Attack Affected More Customers than First Thought*, L.A. TIMES, June 17, 2011, at B1, *available at* http://articles.latimes.com/2011/jun/17/business/la-fi-citigroup-hacking-20110617.

gas companies, water and sewage companies, and transportation companies bear an even higher risk due to the potential catastrophic results. In 2011, hackers took over U.S. satellites on at least two occasions and targeted their command-and-control systems.[11] In both instances, "[t]he responsible party achieved all steps required to command the satellite but did not issue commands."[12] In 2007, a test conducted by scientists at the Idaho National Laboratory demonstrated that an electric generator could be programmed to shake itself to pieces after it was fed hacked instructions.[13] In April 2009, reports emerged stating that China and Russia had infiltrated the U.S. electrical grid and left behind software programs capable of disrupting the system.[14] The North American Electric Reliability Corporation has even publicly warned that the electrical grid is not adequately protected from cyber attack.[15]

President Barack Obama has declared that "America's economic prosperity in the twenty-first century will depend on cybersecurity."[16] The role of the government in cyberspace is complicated, however, since a majority of critical infrastructure and large financial companies are privately owned and controlled. While the U.S. government has tried to assume the role of defender, seeking to prevent attacks on the private sector by prosecuting the culprits and developing military cyber defense capabilities, experts warn that these defense capabilities have fallen far behind the technological prowess of our adversaries.[17] Many nations have developed cyber offensive capabilities that can repeatedly breach, disrupt, and destroy computer networks and the data they contain.[18] America's increasingly sophisticated enemies now include technologically advanced governments, terrorist groups, and even individual hackers.[19] The federal government can no longer afford to ignore the cyber threats that these enemies are capable of perpetrating.

11. *See* Jason Ryan, *US Satellites Compromised by Malicious Cyber Activity*, ABC NEWS, Nov. 16, 2011, http://abcnews.go.com/blogs/politics/2011/11/us-satellites-compromised-by-malicious-cyber-activity

12. *Id*. (internal quotation marks omitted).

13. STEWART BAKER, SHAUN WATERMAN & GEORGE IVANOV, MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 10 (2009).

14. Siobhan Gorman, *Electricity Grid In U.S. Penetrated By Spies*, WALL ST. J., Apr. 8, 2009, at A1, *available at* http://online.wsj.com/article/sb123914805204099085.html.

15. Pub. Notice from Michael Assante, Chief Sec. Officer of the N. Am. Elec. Reliability Corp., (Apr. 7, 2009), *available at* http://online.wsj.com/public/resources/documents/cip-002-identification-letter-040609.pdf.

16. LIPMAN REPORT, *supra* note 7, at 1.

17. *Id*.

18. BAKER, WATERMAN & IVANOV, *supra* note 13, at 5 (citing McAfee's 2007 Virtual Criminology Report).

19. LIPMAN REPORT, *supra* note 7, at 1.

This Note addresses the federal government's role in protecting the private sector's cybersecurity by illustrating the need for, and the potential success of, federal cybersecurity regulations. Part I defines key terms and explains the technical processes used to facilitate a cyber attack. Part II discusses unique characteristics of cyber attacks, including the problem of attacker anonymity, the prevalent use of cyber attacks by non-state actors, and the economic consequences. Part III will delve into the unique threats to national security posed by cyber attacks. Part IV then examines federal initiatives to enhance cybersecurity. Part V will address why the current federal efforts are insufficient and why federal regulations are necessary. Part VI will recommend the creation of a federal cybersecurity agency.

## II. DEFINING CYBERSPACE, CYBER WARFARE, AND CYBER ATTACKS

Cyberspace has a language all its own. Understanding this information-technology ("IT") vernacular and some of the technical processes associated with cyber attacks is critical to understanding cybersecurity.[20]

### A. CYBERSPACE: THE NEW BATTLEFIELD

"Cyberspace is not a physical place—it defies measurement in any physical dimension or time space continuum."[21] Accordingly, there is no internationally accepted definition of "cyberspace." One scholar describes it as, "an evolving man-made domain for the organization and transfer of data using various wavelengths of the electromagnetic spectrum." [22] Another scholar explains, "It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[23] A daunting characteristic of cyberspace is the nearly universal interconnectivity of network systems, regardless of their use. This new interconnectivity has greatly improved the utility of information systems, yet it has also made them more vulnerable to cyber attacks.

20. The importance of understanding this new-era language even motivated Webster to publish a "Hacker's Dictionary." BERNADETTE SCHELL & CLEMENS MARTIN, WEBSTER'S NEW WORLD HACKER DICTIONARY (2006).

21. THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 17 (2000).

22. Major Graham H. Todd, *Armed Attack In Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 68 (2009). The author developed this definition with Major Noah Bledstein. *Id*. at 68 n.5.

23. WINGFIELD, *supra* note 21, at 17.

## B. CYBER WARFARE

As with the term cyberspace, there is no universally accepted definition of "cyber warfare." While some associate this term with a high volume of cyber attacks against a particular target by a hacker or group of hackers, most scholars have limited cyber warfare to be the use of cyber attacks by a country for military purposes.[24] Government security expert Richard Clarke defines it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[25]

States have been forthright about their intentions to build up and use national cyber-warfare capabilities. Today, many states in the international arena are focusing more energy and money on developing their cyber-warfare capabilities. Approximately 120 countries currently have or are developing offensive cyber attack capabilities.[26]

## C. CYBER ATTACKS: DEFINING THE WEAPONS OF CYBER WAR

The Department of Defense defines "computer network attacks" as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[27] Cyber attacks generally consist of one or more of the following methods: directed intrusions into computer networks to steal or alter information; malicious code, known as malware, that propagates from computer to computer and disrupts their functionality; or "denial of service" attacks that bombard networks with bogus communications preventing them from functioning properly.

### 1. Malware

The most widely reported form of cyber attack is by malicious software, or "malware."[28] During this type of attack, hackers find exploitable vulnerabilities in a computer's security system and force access

24. STEVEN A. HILDRETH, CONG. RESEARCH SERV., RL30735, CYBERWARFARE 3 (2001), *available at* http://www.fas.org/irp/crs/RL30735.pdf.

25. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT, 6 (2010).

26. Julian Hale, *NATO Official: Cyber Attack Systems Proliferating*, DEFENSE NEWS, Mar. 23, 2010, http://www.defensenews.com/story.php?i=4550692.

27. JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY & ASSOCIATED TERMS 141 (2010), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

28. BAKER WATERMAN & IVANOV, *supra* note 13, at 6.

into the network and its protected data.[29] Software and instructions for "computer system break-ins" are easily available on the Internet.[30] In addition, software flaws unknown to manufacturers are available on the black market through "bug hunters," or cybersecurity experts who are skilled in discovering and exploiting these vulnerabilities.[31] Malware also provides hackers with tools to disrupt normal computer functions. Commonly used malware include viruses, worms, and Trojan horses.

A "computer virus" is a malicious computer program that attaches itself to an innocuous file in order to spread to other computers.[32] A user simply has to open the malware in order to infect a computer.[33] The virus then multiplies, making many copies of itself, which then spread across networks rapidly.[34] The virus designer can also program the virus to have malicious side effects, such as data destruction.[35] Viruses can be programmed to have immediate effects or they can involve a time delay.[36]

A "worm" is similar to a virus, however it does not require user action to infect a computer.[37] Worms are also able to replicate themselves on a system.[38] They quickly multiply and use up system memory, resulting in network servers and computers becoming overwhelmed and ceasing to respond.[39] Worms also can be programmed to allow remote computer access.[40]

A "Trojan horse" is a program in which harmful code is contained inside apparently harmless programming in order to gain control and then cause damage.[41] Trojan horses have the capacity to destroy important data stored on a network.[42] While Trojan horses also have the capability of allowing remote users access to the compromised network, they do not

29. Phillip W. Brunst, *Use of the Internet by Terrorists—A Threat Analysis*, *in* RESPONSES TO CYBER TERRORISM 38 (Ctr. of Excellence Defence Against Terrorism, Ankara, Turk. ed. 2008).
30. *Id*.
31. Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. 3, ¶¶ 17–18.
32. Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 136 (2009).
33. *Id*. at 136.
34. *Id*. at 135.
35. *Id*. at 135–36.
36. *Id*.
37. *Id*. at 136.
38. *Id*.
39. *Id*.
40. *Id*.
41. *Id*.; Wolfgang McGavran, Comment, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259, 263 (2009).
42. Schaap, *supra* note 32, at 136.

have the ability to self-replicate.[43]

Once access to the computer system is gained, hackers may take actions to disrupt or destroy the network. The easiest course of action is simply to shut down the network.[44] While this can be remedied by turning the network back on, even a brief interruption of some networks, such as control systems for power plants, air traffic control, and electrical grids, can have catastrophic effects.[45]

Hackers may also use the gained access to alter information available on the network to mislead its legitimate users.[46] "Defacements" occur when one webpage is replaced with another that informs the visitor that the website has been compromised and who is responsible for the attack.[47] Hackers may also use the opportunity to destroy data stored on the network.[48] This is a particularly powerful result, especially when the hacker is able to gain access to government databases, top-secret military documents, sensitive nuclear research, or financial institution records.[49]

2. Denial of Service ("DoS")

Even if the hackers are unable to gain access to the network, they are able to cause damage through Denial of Service ("DoS") attacks. A distributed DoS ("DDos") attack involves the use of a large number of malware-infected computers known as "zombies" to simultaneously visit a website in an effort to saturate the server, shutting it down.[50]

A "zombie" is a compromised computer that can be remotely controlled by someone else.[51] An attacker usually gains control by infecting the computer with a virus. A "botnet" is a group of zombies controlled by an outside source.[52] Owners of zombie computers are usually unaware that they are part of a botnet since their computers appear to operate normally.[53]

43. *Id*.
44. Brunst, *supra* note 29, at 38.
45. *Id*.
46. *Id*. at 38–39.
47. *Id*.
48. *Id*. at 39.
49. *Id*.
50. *See* Mindi McDowell, *Cyber Security Tip ST04-015, Understanding Denial Of Service Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/cas/tips/ST04-015.html (last updated Nov. 4, 2009).
51. Michael Ena, Comment, *Securing Online Transactions: Crime Prevention Is the Key*, 35 FORDHAM URB. L.J. 147, 157 (2008).
52. *See* Mindi McDowell, *Cyber Security Tip ST06-001, Understanding Hidden Threats: Rootkits And Botnets*, U.S. COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/cas/tips/ST06-001.html (last updated Aug. 24, 2011).
53. *Id*.

DDoS attacks are widely used by hackers, especially against larger targets, like governments. In February 2011, antigovernment protesters in Egypt used DDoS attacks to shut down the Egyptian government's websites.[54] In 2007, DDoS attacks in Estonia crippled the nation's information systems for weeks,[55] affecting a range of government websites,[56] news organizations, and major banks.[57] The cyber attack cost the Baltic state around €19 million.[58] In July 2008, the country of Georgia also fell victim to a DDoS cyber attack.[59] In just a few days, most Georgian governmental websites were rendered inoperable.[60] In addition, the national bank of Georgia's website was defaced and replaced with images of twentieth-century dictators and Georgia's president.[61]

## III. THE UNIQUE THREATS TO NATIONAL SECURITY POSED BY CYBER ATTACKS

### A. THE DISTINCTION BETWEEN KINETIC WAR AND CYBER WARFARE

The Supreme Court once described war as "the exercise of force by bodies politic . . . against each other, for the purpose of coercion."[62] With cyberspace as the new battlefield, traditional warfare has been turned on its head. As Major Graham H. Todd stated, "[s]imply put, information is fundamentally different than the traditional tools of war; bits and bytes bear no resemblance to bullets and bombs."[63]

Michael Schmitt notes that cyberspace threats differ in four ways from traditional threats: (1) While computer networks are a new target category, network attacks are capable of providing the same results as striking the traditional target with a kinetic weapon; (2) an attack does not have to use kinetic force and can involve a command from one computer; (3) the

54. Ravi Somaiya, *Hackers Shut Down Government Sites*, N.Y. TIMES, Feb. 2, 2011, http://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html.

55. *Estonia Hit by 'Moscow Cyber War,'* BBC NEWS, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

56. *Id*.

57. Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 61 (2010).

58. Mallet, *supra* note 5.

59. Lieutenant Colonel Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 46 (2009).

60. *Id*.

61. John Markoff, *Georgia Takes a Beating in the Cyberwar with Russia*, N.Y. TIMES BITS BLOG (Aug. 11, 2008, 9:20 PM), http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia.

62. The Brig Amy Warwick (The Prize Cases), 67 U.S. 635, 652 (1863).

63. Todd, *supra* note 22, at 68.

intended results are often not kinetic and involve the manipulation of data or disruption of a service; and (4) cyberspace threats are not constrained by political boundaries or geography.[64]

The final distinction is perhaps the most important. The global nature of telecommunications networks means that cyber attacks can be launched from anywhere in the world, at low cost, and with incredible speed. Furthermore, it is nearly impossible to predict in advance when an attack may begin.[65]

Major Graham H. Todd adds additional distinguishing factors to Schmitt's list. He notes that: (1) cyberspace attacks can be completed literally at the speed of light;[66] (2) the cost of acquiring the equipment and expertise to conduct operations in cyberspace is de minimis in comparison to fielding conventional forces; and (3) attributing the attack to the responsible party and determining whether the attack was intentional is extremely difficult.[67] These factors demonstrate the heightened peril of cyber attacks.

### B. THE PROBLEM OF ANONYMITY AND THE RISE OF NON-STATE ACTORS

A hacker's ability to program a computer to infiltrate other computers creates a layered system, enabling the cyber culprit to hide behind botnets and innocent third parties.[68] Current technology is inadequate to trace these malware back to their original source. As a former U.S. law enforcement official stated, "[e]ven if you can trace something back to a [computer], that doesn't tell you who was sitting behind it."[69] This inability to identify the attacker gives hackers "plausible deniability," allowing them to avoid punishment since there is insufficient evidence to prove an allegation.[70] This makes it difficult to bring the criminals to justice or deter others from committing the same crime.[71]

64. Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on Normative Framework*, 37 COLUM. J. OF TRANSNAT'L LAW 885 (1999).

65. Katharina von Knop, *Institutionalization of a Web-Focused, Multinational Counter-Terrorism Campaign—Building a Collective Open Source Intelligent System*, *in* RESPONSES TO CYBER TERRORISM 8 (2008).

66. As one scholar put it, there is no longer "the luxury of the twenty-minute window from launch to landing of a nuclear-tipped intercontinental ballistic missile as there was in the Cold War." *Id*. at 9.

67. Todd, *supra* note 22, at 68–69.

68. BAKER, WATERMAN & IVANOV, *supra* note 13, at 6.

69. Eric Talbot Jensen, *Cyber Warfare and Precautions Against The Effects of Attacks*, 88 TEX. L. REV. 1533, 1538 (2010) (quoting BAKER, WATERMAN & IVANOV, *supra* note 13, at 6).

70. *Id*.

71. Toby L. Friesen, *Resolving Tomorrow's Conflicts Today: How New Developments Within The U.N. Security Council Can Be Used To Combat Cyberwarfare*, 58 NAVAL L. REV. 89, 103 (2009).

The low cost, ease and "masking effect" of cyber attacks make their use appealing to non-state actors. Some of these non-state actors include individual hackers, political or "hacktavist" [72] groups, and terrorist organizations. Motivations for cyber attacks vary widely. Usually, individual hackers are looking to gain money, information or an increased reputation and prestige. Terrorist and "hacktavist" organizations are generally gleaning to gain vital information on their opponent, or to send a particular message by disrupting an important aspect of the target's daily operations.[73]

## C. ECONOMIC CONSEQUENCES

One of the most distinct characteristics of cyber attacks is their ability to cause catastrophic economic damage using few resources. The computer-security company, McAfee, has stated that the economic damage caused by malicious cyber activities is as high as $1 trillion per year.[74] Economic transactions, particularly in financial markets, are hugely dependant on reliable information and consistent network operations. A direct attack on a financial market has the potential for significant financial consequences. Given current international economic interdependency, an attack on one country's financial market also has the potential to create catastrophic effects for the global economy.[75] The losses could include the destruction of intellectual property, financial fraud, damage to reputation, lower productivity, and third party liability.[76] Investigations into the stock price impact of cyber attacks show that some firms suffer losses of 1 to 5 percent in the days after an attack.[77] For the average corporation listed on the New York Stock Exchange, price drops of these magnitudes translate into losses of between $50 million and $200 million of market capitalization.[78]

72. Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist. *Hacktivism*, SEARCHSECURITY.COM, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci552919,00.html (last visited Apr. 3, 2012).

73. Brunst, *supra* note 29, at 36–37.

74. Obermann, *supra* note 7.

75. Vida M. Antolin-Jenkins, *Defining The Parameters Of Cyberwar Operations: Looking For Law In All The Wrong Places?*, 51 NAVAL L. REV. 132, 145–46 (2005).

76. James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES 5, 6 (Dec. 2002), *available at* http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

77. BRIAN CASHELL, WILLIAM D. JACKSON, MARK JICKLING & BAIRD WEBEL, THE ECONOMIC IMPACT OF CYBER-ATTACKS, *Summary* (CRS Report for Congress 2004).

78. *Id*.

Given the unique characteristics and dire consequences of cyber attacks, the United States has begun to take actions to increase its cybersecurity.

## IV. FEDERAL ACTIONS AIMED AT ENHANCING CYBERSECURITY

President Barack Obama has declared that the threat of cyber attack "is one of the most serious economic and national security challenges we face as a nation."[79] His administration has acknowledged that the U.S. digital infrastructure is not secure enough to withstand today's threats, or those that are likely to come in the future.[80] The Chairman of the House Intelligence Committee also recently warned that the United States will soon suffer a catastrophic cyber attack if it doesn't act now to prevent it.[81]

On February 9, 2009, President Obama directed a sixty-day comprehensive review to assess U.S. cybersecurity policies.[82] This Cybersecurity Policy Review (the "Review") led to recommendations for an increase in research programs, the creation of partnerships with the private sector and the IT workforce, the creation of an effective information sharing and incident response system, and increased encouragement of innovation.[83]

In February 2010, the House of Representatives, in response to the Review, approved the Cybersecurity Enhancement Act of 2010 (the "Act").[84] The Act is meant to enhance cybersecurity through improving the transfer of cybersecurity technologies to the marketplace, training an IT workforce for both the public and private sectors, and coordinating federal

79. Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

80. *Homeland Security*, THE WHITE HOUSE, http://www.whitehouse.gov/issues/homeland-security (last visited Apr. 3, 2012).

81. Pam Benson, *Catastrophic Cyberattack Looms*, CNN SECURITY CLEARANCE BLOG (Feb. 2, 2012, 4:23 PM), http://security.blogs.cnn.com/2012/02/02/catastrophic-cyberattack-looms.

82. THE WHITE HOUSE, CYBERSPACE POLICY REVIEW (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [hereinafter CYBERSPACE POLICY REVIEW]. To enhance the cybersecurity of the private sector, the Review recommended creating public-private partnerships centered on information sharing. *Id*. at vi. The Review also suggested that officials work with the private sector to examine existing public-private information sharing mechanisms to identify the most effective models. *Id*. at 17. In addition, the Review encouraged the federal government to consider options for incentivizing collective action and enhancing competition in the development of cybersecurity solutions. *Id*. at 28. Recommended incentives included adjustments to liability considerations, indemnification, tax incentives, and new regulatory requirements and compliance mechanisms. *Id*.

83. *Id*.

84. Cybersecurity Enhancement Act of 2010, H.R. 4061, 111th Cong. (2010).

cybersecurity research and development.[85] While the Act passed the House, it has made modest headway in the Senate. Despite the President's recommendations, little has actually been done to create these partnerships or incentives.

In 2011, members of both parties in Congress recognized the urgent need for stronger cybersecurity legislation and approximately 50 cyber-related bills were introduced.[86] In May 2011, the Obama Administration, recognizing that "our Nation cannot fully defend against these threats unless certain parts of cybersecurity law are updated," [87] issued a Cybersecurity Legislative Proposal (the "Proposal") at the request of Congress. In additional to suggesting various voluntary information sharing and government assistance programs, the Proposal nominated the Department of Homeland Security ("DHS") to work with industry to identify the core critical-infrastructure operators and to prioritize the most important cyber vulnerabilities.[88] Each of those operators would develop its own frameworks for addressing cyber threats, which would then be reviewed by a third-party commercial auditor.[89] Should an auditor deem a plan insufficient, the DHS could work with the operator to improve the plan.[90]

In response to the Proposal, on February 1, 2012, a House Homeland Security Subcommittee passed the Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011 (the "PrECISE Act").[91] The PrECISE Act gives the Secretary of Homeland Security a leading role in improving the nation's cybersecurity. The DHS is made responsible for maintaining a clearinghouse of cyber threat information and disseminating that information to the federal government as well as the private sector.[92] The PrECISE Act also creates a nonprofit corporation, the National Information Sharing Organization to manage the private-to-private aspects of cyber threat information sharing.[93]

85. 156 CONG. REC. E 175, (Feb. 22, 2010) (speech by Hon. Sheila Jackson Lee in the House of Representatives).

86. Press Release, THE WHITE HOUSE, *Fact Sheet: Cybersecurity Legislative Proposal*, May 12, 2011, http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

87. *Id*.

88. *Id*. (under "Protecting our Nation's Critical Infrastructure").

89. *Id*.

90. *Id*.

91. The PrECISE Act of 2011, H.R. 3674, 112th Cong. (2011).

92. *Id*. at 1–22.

93. *Id*. at 23–45. NISO would be managed by a joint public-private board of directors with additional representation from privacy and civil-liberties nongovernmental organizations.

On February 14, 2012, Senators John Rockefeller, Dianne Feinstein, Susan Collins, and Joseph Lieberman introduced the comprehensive Cybersecurity Act of 2012[94] that, similar to the PrECISE Act, requires the Secretary of Homeland Security to designate certain infrastructure as critical and to compel steps to safeguard against hackers.[95] Some political analysts state that the bill would impose mandatory standards, giving it a bit more regulatory bite than PrECISE's light, information-sharing approach.[96] However, an expert familiar with the legislation dubbed it "a very gentle bill with minimal means for DHS to enforce the new cybersecurity standards."[97]

While these efforts by the federal government are a significant step towards increasing cybersecurity in the private sector, they are far from complete in achieving that goal.[98] The next section of this Note will explain the need for stronger federal regulation and auditing of private-sector cybersecurity.

## V. THE NEED FOR STRONGER FEDERAL CYBERSECURITY REGULATION OF AMERICA'S PRIVATE INDUSTRIES

Everyday, hundreds of attempted cyber attacks are made on the nation's private networks, threatening crucial industries, institutions and government agencies. The federal government, however, has taken inadequate steps to enhance our cybersecurity. This section will demonstrate that national security, economic concerns and a lack of business incentives necessitate tougher federal cybersecurity regulations. It will also discuss the success of cybersecurity regulations in other countries.

94. The Cybersecurity Act of 2012, S. 2105 (Feb 14, 2012).

95. Diane Bartz, *Senators Launch New Push for Cybersecurity Bill*, MSNBC, (Feb. 14, 2012), http://www.msnbc.msn.com/id/46384534/ns/technology_and_science-security/t/senators-launch-new-push-cybersecurity-bill.

96. Nagesh Gautham, *Senate Cybersecurity Bill Sparking Concerns about Government Control*, THE HILL (Jan 29, 2012, 2:38PM), http://thehill.com/blogs/hillicon-valley/technology/207255-senate-cybersecurity-bill-sparking-concerns-about-government-control; Chris Strohm & Eric Engleman, *Obama Pushes Cyber Bill*, BLOOMBERG (Feb 1, 2012), http://www.treasuryandrisk.com/2012/02/01/obama-pushes-cyber-bill.

97. Strohm & Engleman, *supra* note 95.

98. In addition to these security enhancement initiatives, the federal government has also taken action to enhance the prosecution of cyber criminals. In 1984, Congress enacted the Computer Fraud and Abuse Act ("CFAA"). Computer Fraud and Abuse Act of 1984, 98 Pub. L. No. 473, § 2102(a) (1984). The law governs "protected computers," which means any computer used in interstate commerce or communications, including computers used by private parties. Ena, *supra* note 51, at 167. The CFAA was further enhanced by the Computer Software Privacy and Control Act of 2003, which made it a criminal act to knowingly transmit a computer program, code, or command that results in damage to a protected computer, regardless of whether or not access to the computer was authorized. *Id*. at 168.

### A. NATIONAL SECURITY AND ECONOMIC CONCERNS NECESSITATE FEDERAL CYBERSECURITY REGULATIONS

Cyber attacks aimed at the American private sector directly affect the national security of the United States. The susceptibility of America's critical infrastructure, including electrical grids, satellites, and oil, gas, water and transportation companies, is high and the possible consequences are devastating. As the security company McAfee describes it, "[m]any . . . critical infrastructures were built for reliability and availability, not for security. Traditionally, these organizations have had little to no cyber protection, and have relied on guards, gates and guns."[99]

In 2011, it was announced that hackers in China had infiltrated the computer systems of several major U.S. oil, energy, and petrochemical companies. Since November 2009, covert cyber attacks have been launched against these companies in order to acquire confidential information on oil and gas field operations.[100] Hackers have also installed remote administration software on the companies' networks, allowing them to wield control of the systems.[101] McAfee's chief technology officer warns that "[w]ell-coordinated, targeted attacks . . . orchestrated by a growing group of malicious attackers . . . are rapidly on the rise."[102] These recent attacks on the oil and gas sector, as well as the electrical grid incidents mentioned earlier, demonstrate the pressing need for government regulation of private industries' cybersecurity.

The interconnectedness of the civilian, government and military networks exacerbates the danger of cyber attacks on American networks. As the public adopts each new generation of IT, use by government correspondingly increases. Federal, state, and local authorities now use these technologies and networks for routine administrative functions, improving services and access to government information. The federal government also employs IT for critical functions like foreign affairs, military command, and intelligence efforts. In fact, a staggering 98 percent of all U.S. government communications travel over civilian networks,[103] and an estimated 95 percent of military information pass through civilian

99. Press Release, *McAfee, Inc. Report Reveals Cyber Coldwar, with Critical Infrastructure Under Constant Cyberattack Causing Widespread Damage*, MCAFEE (Jan. 28, 2010), http://www.mcafee.com/us/about/news/2010/q1/20100128-01.aspx.

100. Robert Perkins, *Chinese Hackers Target Oil, Gas Majors in Growing Cyber-Attack*, PLATTS, (Feb. 10, 2011), http://www.platts.com/RSSFeedDetailedNews/RSSFeed/Oil/8526266.

101. *Id*.

102. George Kurtz, *Global Energy Industry Hit in "Night Dragon" Attacks*, MCAFEE BLOG, (Feb. 9, 2011, 9:18PM), http://blogs.mcafee.com/corporate/cto/global-energy-industry-hit-in-night-dragon-attacks.

103. Jensen, *supra* note 69 , at 1534.

networks.[104] The interconnectivity of civilian and government networks provides hackers with the ability to disrupt important government and military functions simply by hacking into a private network. In just the early months of 2012, both the Department of Justice and the Federal Bureau of Investigation have experienced crippling cyber attacks.[105] Thus, the susceptibility of America's critical infrastructure and civilian networks presents a real danger to national security.

The private sector's cyber vulnerabilities also threaten the American economy. As discussed earlier, cyber attacks generally have staggering economic consequences. The reported cost of downtime from major attacks exceeds $6 million per day.[106] In the oil and gas sector, that estimate jumps to $8.6 million per day.[107] Recently, cyber attacks have even threatened the stock market. In February 2011, the financial world erupted in shock as the Nasdaq Stock Market announced that hackers had penetrated its system.[108] While the exchange's trading platform wasn't compromised, the attack affected a Nasdaq subsidiary, which offers web-based tools for roughly 10,000 clients including well-known, publicly traded companies.[109] While some fear that the illegal access will enable hackers to view confidential information, aiding them in making lucrative stock transactions, many are apprehensive that such actions are only a few steps away from accessing the trade platform itself, causing a national, or worse, global financial crisis.[110] This threat to the American financial system further demonstrates the need for tougher federal regulation of private networks.

### B. LACK OF BUSINESS INCENTIVES COMPELS PRIVATE CYBERSECURITY REGULATION

Business incentives, which generally play an important role in companies' decisionmaking processes, have proven insufficient in encouraging an increase in cybersecurity. While security and profitability may be intertwined, since a lack of security can impact economic performance, company initiatives to increase cybersecurity are ultimately

104. Antolin-Jenkins, *supra* note 75, at 132–133.

105. *Department of Justice Site Hacked After Megaupload Shutdown, Anonymous Claims Credit*, WASH. POST, Jan. 20, 2012, http://www.washingtonpost.com/business/economy/department-of-justice-site-hacked-after-megaupload-shutdown-anonymous-claims-credit/2012/01/20/gIQAl5MNEQ_story.html; Jerry Brito, *FBI Hacked While Congress Ponders Cybersecurity Legislation*, TIME, Feb. 6, 2012, http://techland.time.com/2012/02/06/fbi-hacked-while-congress-ponders-cybersecurity-legislation/.

106. BAKER, WATERMAN & IVANOV, *supra* note 13, at 3.

107. *Id*. at 10.

108. *See* Devlin Barrett, *Hackers Penetrate Nasdaq Computers*, WALL ST. J. TECH., Feb. 5, 2011, http://online.wsj.com/article/sb10001424052748704709304576124502351634690.html.

109. *Id*.

110. *Id*.

subordinated to profitability considerations. Even the government has acknowledged that "[t]he private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security into corporate risk management."[111]

This "return on investment" mentality and its negative effects on cybersecurity are readily visible in American companies' corporate strategy decisions. A recently released Bloomberg Government study found that utilities, banks and other infrastructure operators would need to increase their expenditures on cybersecurity by almost nine times in order to prevent 95 percent of cyber attacks.[112] However, the study also revealed that although "the threats and costs are going up . . . the investments are going down," and that the gap between the two "is much higher than [they] had expected."[113] In addition, a report published by the Center for Strategic and International Studies ("CSIS") and McAfee ("CSIS Report") surveyed 600 security and IT executives in fourteen countries about their practices, attitudes and policies on cybersecurity.[114] Two-thirds of executives surveyed said there were cuts in their company's cybersecurity resources as a result of the recession.[115] Furthermore, 35 percent of the American executives stated that these cuts had reduced their security resources by 15 to 25 percent.[116] Surprisingly, the energy and oil sectors had the most widespread security cuts, with 75 percent of the respondents reporting reductions.[117] Thus, the "return-on-investment" mentality, coupled with the recent financial crisis, has led to reduced cyber protections, a change the federal government should not tolerate.

### C. REGULATIONS HAVE PROVEN TO BE SUCCESSFUL IN INCREASING CYBERSECURITY

The CSIS Report also revealed data about the effectiveness of government regulations in improving cybersecurity. To date, China has the highest level of regulatory and legislative activity by the government, with 92 percent of executives stating that they were subject to cybersecurity laws and regulations.[118] Surprisingly, American executives reported the *lowest* levels of regulatory activity.[119] While American executives voiced

111. *Cyberspace Policy Review*, *supra* note 82, at 17.
112. *See* Strohm & Engleman, *supra* note 95.
113. *Id*.
114. BAKER, WATERMAN & IVANOV, *supra* note 13, at 1.
115. *Id*. at 14.
116. *Id*. at 15.
117. *Id*. at 14.
118. *Id*. at 28.
119. *Id*. (emphasis added).

concern that "regulation is a lot of useless activity at great cost,"[120] the statistics collected told a different story. In countries where there were regulations, such as Brazil, Spain, China, Mexico, Germany and Japan, more than 60 percent of the executives surveyed agreed that the regulations had improved security.[121] Seventy-four percent said their organization had "implemented new policies, procedures, best practices or technical measures" as a direct result of regulation.[122] In China, a staggering 91 percent of surveyed executives said their companies had changed policies because of government legislation.[123]

While regulations proved critical to creating cybersecurity policies, the CSIS Report also revealed that auditing plays an important role. While both China and India reported high levels of regulation, only China demonstrated an increase in cybersecurity procedures as a result of the laws.[124] One of the noticeable differences between the two countries was the level of auditing by government agencies. Over 80 percent of Chinese executives surveyed reported auditing by the government, while only 40 percent of the Indian executives reported auditing.[125] A mere 40 percent of American executives also reported auditing by a government agency.[126]

While China's example provides strong evidence of the beneficial results of cybersecurity regulations and auditing, some experts doubt that the results in China are easily duplicated.[127] These experts cite to China's authoritarian state and culture as contributing factors.[128] While this may be true, the CSIS Report still provides strong evidence that such regulations do, in fact, result in better cybersecurity. A solid majority of the executives surveyed from all fourteen countries believe that regulation and/or legislation has improved cybersecurity.[129]

## VI. NECESSARY GOVERNMENT ACTION: A FEDERAL CYBERSECURITY AGENCY

This Note has demonstrated the urgent need for tougher federal cybersecurity regulations. This section will first suggest that Congress

120. *Id*. at 29.
121. *Id*. at 27.
122. *Id*. at 26–27.
123. *Id*. at 27.
124. China reported 91 percent while India reported only 66 percent. *Id*. at 21.
125. *Id*. at 29.
126. *Id*.
127. *Id*. at 39.
128. *Id*.
129. *Id*. at 27.

should create a federal cybersecurity agency, solely responsible for promulgating tougher cybersecurity rules and auditing companies' compliance. It will then articulate what the tougher policies and standards should look like.

Many have questioned the government's ability to draft effective cybersecurity regulations.[130] As one analyst put it, "[t]he threat changes so fast, technology changes so fast, . . . there is no way government regulation can ever keep up."[131] American executives have also voiced concern about "the government's knowledge of what should be done and a lack of knowledge on the part of the government of the operation of the various infrastructures."[132] Nonetheless, the creation of a federal cybersecurity agency, responsible for the construction and enforcement of cybersecurity regulations is the best and most efficient manner to alleviate this fear while ensuring successful cybersecurity regulations.

The U.S. Government Accountability Office ("GAO") provides an excellent model of how the new federal agency should be structured. The GAO, also known as the "congressional watchdog," is solely responsible for investigating how the federal government spends taxpayer dollars.[133] The GAO also advises Congress and the heads of executive agencies about ways to make government more efficient, effective, and ethical.[134] In order to make these assessments, the GAO is responsible for researching and understanding how each government agency works. In addition, the GAO supports congressional oversight by auditing agency operations to determine whether federal funds are being spent efficiently, reporting on how well government programs and policies are meeting their objectives, and issuing legal decisions and opinions.[135]

Similar to the GAO, the new cybersecurity agency should be the sole entity responsible for enhancing America's cybersecurity—a "cyber watchdog," if you will. The agency will conduct research on the inner-workings of the various infrastructures and their networks, as well as possible security solutions, and publish conclusions based on its findings. It will then promulgate regulations for each industry aimed at enhancing the cybersecurity of that particular sector while taking into account its distinct

130. *See* John Grant, *National Leadership, Individual Responsibility: Will There Be Cybersecurity Legislation?*, 4 J. NAT'L SECURITY L. & POL'Y 103, 110–12 (2010).

131. Strohm & Engleman, supra note 95.

132. BAKER, WATERMAN & IVANOV, *supra* note 13, at 29.

133. *About GAO*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), http://www.gao.gov/about/index.html (last visited Apr. 3, 2012).

134. *Id*.

135. *Id*.

characteristics, needs, and limitations. In addition, the agency should be responsible for performing policy analyses and providing companies information about various cybersecurity technologies, policies, and strategies. Furthermore, the agency should work with other government entities to create an incentive program aimed at encouraging cybersecurity and innovation. These incentives could include grants for companies that undertake cybersecurity research, or tax benefits for companies that employ higher standards of cybersecurity than those mandated.

As discussed in the prior section, regulations are more effective when they are paired with external auditing and compliance measures. Thus, the new cybersecurity agency, like the GAO, should also be responsible for conducting audits and compliance checks of the private sector's cybersecurity programs. Such audits will also provide a supplementary opportunity to discover vulnerabilities within a company's network or cybersecurity policies.

The new agency should also enact a penalty system aimed at disciplining companies that are not in compliance. In China, when a violation occurs, the government first orders remedial actions within a specific period and issues a warning; if the deadline is not met, then a fine may be assessed against the company.[136] In the case of serious offenses, the network can be closed for up to six months.[137] If necessary, the government may even suggest that the business license or network registration of the organization be canceled.[138] A similar system should be devised by the cybersecurity agency for violations discovered during an audit. Violations that are discovered as a result of a successful cyber attack should result in steeper penalties and fines, and perhaps even liability.

Tougher cybersecurity regulation is necessary due to our critical infrastructures' extreme vulnerability and the lack of business incentives. The Federal Financial Institutions Examination Council ("FFIEC") cybersecurity and IT policies provide an excellent model for the types of policies the new cybersecurity agency should adopt. The FFIEC prescribes principles, standards, and examination procedures to promote consistency

136. China's Computer Information Network and Internet Security, Protection and Management Regulations, Article 21 (promulgated by the Ministry of Public Security on December 30, 1997), *available at* http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html (last visited Apr. 3, 2012).

137. *Id*.

138. *Id*.

in the supervision of financial institutions,[139] and recently established IT regulations and standards.

The FFIEC IT Handbook ("Handbook") provides a framework for the government examination of these institutions' IT infrastructure[140] and guidance for their daily IT and cyber operations.[141] Financial institutions must maintain an ongoing information security risk assessment program that: (1) gathers data regarding the threats and vulnerabilities of their IT assets, existing security controls, processes, standards and requirements; (2) analyzes the probability and impact associated with known threats and vulnerabilities; and (3) prioritizes risks to determine the appropriate level of training and control necessary for effective mitigation.[142] Financial institutions then must develop a cybersecurity strategy and implementation plan. This plan must include appropriate consideration of prevention, detection and response mechanisms and policies to guide employees in implementing the security program.[143] To strengthen compliance with these guidelines, the Handbook prescribes internal audit procedures for financial institutions.[144]

Following the policies in the Handbook, the new DHS component should require companies in all critical infrastructures to adopt policies and practices aimed at identifying, prioritizing, and eliminating vulnerabilities in their networks. Like the FFIEC, new regulations should mandate that companies adopt "security risk assessment programs" where they are required to implement a coherent set of policies to manage risks to their IT assets and operational capabilities.[145] A well-planned internal audit program should also be required. As the FFIEC explains, "[e]ffective audit

139. *About the FFIEC*, THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL ("FFIEC"), http://www.ffiec.gov/about.htm (last visited Apr. 3, 2012).

140. FFIEC IT Examination HandBook InfoBase, *Overview*, FFIEC, http://ithandbook.ffiec.gov/it-booklets/information-security/introduction/overview.aspx (last visited Apr. 3, 2012). *See also* Ena, *supra* note 69, at 171–172.

141. FFIEC IT Examination HandBook InfoBase, *Security Process Overview*, FFIEC, http://ithandbook.ffiec.gov/it-booklets/information-security/security-process/overview.aspx (last visited Apr. 3, 2012).

142. FFIEC IT Examination HandBook InfoBase, *Information Security Risk Assessment*, FFIEC, http://ithandbook.ffiec.gov/it-booklets/information-security/information-security-risk-assessment.aspx (last visited Apr. 3, 2012).

143. FFIEC IT Examination HandBook InfoBase, *Information Security Strategy*, FFIEC, http://ithandbook.ffiec.gov/it-booklets/information-security/information-security-strategy.aspx (last visited Apr. 3, 2012).

144. FFIEC IT Examination HandBook InfoBase, *Audit Introduction*, FFIEC, http://ithandbook.ffiec.gov/it-booklets/audit/introduction.aspx (last visited Apr. 3, 2012).

145. For a discussion on the use of Security Information Management Systems see Gurpreet Dhillon & James Backhouse, *Information System Security Management in the New Millennium*, Technical Opinion, COMMUNICATIONS OF THE ACM Vol. 43, No. 7 (July 2000), *available at* http://tols17.oulu.fi/~jhyvonen/Tietoturvan%20hallinta%20tenttimateriaalit/Luento1.pdf.

programs are risk focused, promote sound IT controls, ensure the timely resolution of audit deficiencies, and inform the board of directors of the effectiveness of risk management practices."[146] Similar to the requirements of the FFIEC,[147] companies should be able to outsource their internal audits to outside IT firms, provided that the firms meet certain requirements.

As studies have shown, tougher regulation of critical infrastructure's cybersecurity paired with a system of auditing and accountability have the ability to greatly enhance the security of our nation and its networks. Congress would be well advised to create a federal cybersecurity agency. Such a specialized agency would be better adept at understanding each industry's cybersecurity vulnerabilities and needs, promulgating specialized mandatory regulations and standards for different sectors, and conducting thorough inspections of companies' cybersecurity policies and actions.

## VII. CONCLUSION

The threat of a catastrophic cyber attack against the United States' critical infrastructure is real and continually growing more perilous. Networks controlling the nation's most crucial infrastructure receive thousands of hacking attempts—many successful—every year. Yet market forces, the inability to determine the identity of the attacker, and a lack of federal regulations have left these infrastructures vulnerable. Federal cybersecurity regulations and compliance efforts can have positive and lasting effects on the public sector's cybersecurity, as well as national security. The creation of a separate federal agency responsible for promulgating and enforcing cybersecurity regulations would significantly improve online security and greatly reduce the threat of cyber attacks.

146. *Audit Introduction*, *supra* note 143.

147. *See* FFIEC IT Examination HandBook InfoBase, FFIEC, *Outsourcing Internal IT Audit*, FFIEC, http://ithandbook.ffiec.gov/it-booklets/audit/outsourcing-internal-it-audit.aspx.