5-1-2014

Unrestricted Warfare: The Rise of a Chinese Cyber-Power

Robert John Guanci

Unrestricted Warfare:

The Rise of a Chinese Cyber-Power

Robert Guanci

"We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy. "[1]

On January 30, 2013, the New York Times reported that its computer databases had been infiltrated.[2] As a result, personal emails, lists of journalists and dozens of contacts and files had been compromised. That same week it was reported that Bloomberg news, the Wall Street Journal, as well as the Washington Post had all been victims to similar attacks to their cyber infrastructure.[3] Similarly, ten years earlier, a sophisticated and coordinated "cyber-espionage" ring code-named "Titan Rain" swept across some of the U.S. government's most sensitive agencies.[4] NASA, the Department of Defense, (DOD), and the Department of Homeland Security, (DHS) fell victim to a massive "cyber-attack" resulting in the theft of enormous amounts of data.[5]

While in neither of these cases has it been conclusively proven, there exists a growing consensus among U.S. politicians, lawmakers, and military officers that the origins of these attacks, as well as others, stem from China.[6] For example, in the aftermath of the New York

---

[1] Ellen Nakashima, Obama orders voluntary security standards for critical industries' computer networks, Wash. Post, Feb. 12, 2013, at 1.
[2] Nicole Perlroth, Washington Post Joins List of News Media Hacked by the Chinese, N. Y. Times, Feb. 1, 2013, at 1.
[3] Id. at 1.
[4] 1 Kirsten M. Koepsel, Electronic Security Risks and the Need for Privacy, *in* State-sponsored threats from the Peoples Republic of China (PRC), Data Sec. & Privacy Law § 1:19 1,1 (2012).
[5] Id. at 1.
[6] William Wan & Ellen Nakashima, Report ties cyberattacks on U.S. computers to Chinese military, Wash. Post, Feb. 19, 2013, at 1.

Times attack earlier this year, red flags were raised as evidence surfaced showing that the New York Times' newsroom computers had been in communication with web servers traced back to China.[7] As it turns out, these "cyber-attacks" were not an aberration, the New York Times, as well as other media outlets experienced similar incidents in 2012 and prior years.[8]

Some security experts argue that Chinese hackers started targeting U.S. news media as early as 2008 in an effort to monitor American coverage of Chinese politics.[9] The timing of these breaches in security coincided with a New York Times article on October 25, 2012, detailing the accumulating fortune of Wen Jiabao, China's then President, and his relatives.[10] As it turns out, Bloomberg News published a similar story in 2012 about Xi Jinping and his accumulating fortune.[11] To accomplish this feat, the hackers stole the passwords of every Times employee to access the personal computers of fifty-three employees.[12] It was revealed that the hackers sought information that was only related to the Wen Family story.[13]

Overall, the threat of "cyber-crime" is ubiquitous in today's modern Internet age. Threats to one's personal identity –including email accounts, bank accounts and other personal information are commonplace and as a result, a multi-million dollar industry has risen to the task to provide everyday citizens a way to safeguard their personal information online. However, while the private sector has taken it upon itself to market cybersecurity to private citizens, it has become abundantly clear that the same sort of security is lacking in regards to legislation

[7] Perlroth, *supra* note 2, at 1.
[8] Id. at 1.
[9] Id. at 1.
[10] Nicole Perlroth, Hackers in China attacked the Times for last 4 months, N.Y. Times, Jan. 30, 2013, at 1.
[11] Nakashima, *supra* note 2, at 1.
[12] Id. at 1.
[13] Id. at 1.

designed to address these threats to the United States as a whole –threats to the government, economy, as well as the military.[14]

As a result, the United States government and lawmakers have taken notice and thus proffered bills such as, the Cyber-security bill of 2012 to meet the challenges posed by cyber-criminals all over the world.[15] Nevertheless, many in the U.S. government feel that it has become more than a coincidence that after attacks against U.S. media outlets, industry, or the military, everyone's fingers seem to point to China.[16] While the Russians, Iranians, or even non-state actors are often reported perpetrators of "cyber-attacks," several lawmakers in Washington suggest that the Chinese government has specifically turned its eyes toward the United States –or at least been complicit to the goings-on of citizen-hackers.[17] In fact, the DOD has stated that for the past ten years, it is essentially under continuous attack –citing China as a repeat offender.[18]

To address this dilemma, President Obama on February 12, 2013, issued an executive order calling for increased awareness and a dedication to curtailing any ensuing cyber threats.[19] He proclaimed that the growing threat to the Nation's critical infrastructure, defense, and economic security presents one of the most serious national security challenges facing America today –a challenge he admits can no longer go unnoticed.[20] To that end, this paper will outline the emerging cyber threat facing the U.S. today and offer legal recommendations that should be incorporated into the next cybersecurity legislation to come before Congress.

---

[14] Ellen Nakashima & Danielle Douglass, More companies reporting cybersecurity incidents, Wash. Post, Mar. 1, 2013, at 1.
[15] Chris Finan, Five reasons why Congress should pass Cybersecurity Act of 2012, The Hill's Congress Blog (Nov. 14, 201, 4:00 PM), http://thehill.com/blogs/congress-blog/homeland-security/267945-five-reasons-why-congress-should-pass.
[16] Nakashima, *supra* note 13, at 1.
[17] Ellen Nakashima, U.S. said to be target of massive cyber-espionage campaign, Wash. Post, Feb. 10, 2013, at 1.
[18] Koepsl, *supra* note 4, at 1.
[19] Exec. Order No. 13636, 3 C.F.R. (Feb. 12, 2013).
[20] Id.

Part I of this article will specifically outline the threat that is "cyber-crime." This section will discuss the various tools in the belt of the modern-day hacker, including techniques such as phishing, hacking and Distributed denial-of-service attacks, (DDOS), attacks.[21] Part II of this article will set out the applicable law that governs these attacks. What are the available legal options for the U.S. government or private companies, such as the New York Times, when their networks have been hacked? Are there statutory provisions addressing the issue? Is there a remedy if a foreign hacker hacks a corporation in the United States, but is physically outside of the country?

Part III will outline some of the most recent and noteworthy "cyber-attacks" today. From the hacking of Google to the breach on the DOD, this section will explain why and how China continues to breach U.S. cybersecurity. Finally, the crux of the argument in Part IV will discuss Congress' failure to enact necessary legislation to address the issue. House Homeland Security Committee Chairman, Michael McCaul has said that "cyber-security legislation will be the top legislative priority for the committee next Congress…."[22] If so, why have proffered bills in the past failed before Congress? Therefore, this final section will explain what has kept previous legislative attempts back, and why, in light of the ongoing Chinese "cyber-attacks," Congress must enact a bill to address the current weaknesses in the U.S. cyber-infrastructure.[23]

I. What is "Cyber-Crime?"

In a speech in 2009, President Obama remarked that "our digital infrastructure--the networks and computers we depend on every day--will be treated as they should be: as a strategic

---

[21] Charlotte Decker, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, 81 S. Cal. L. Rev. 959, 965 (2008).

[22] Jennifer Martinez, McCaul: Cybsercurity legislation is top priority next Congress, The Hill's Congress Blog (Dec. 5, 2012, 3:53 PM), http://thehill.com/blogs/hillicon-valley/technology/271251-mccaul-cybersecurity-legislation-is-qtopq-priority-next-congress.

[23] Nathan Gardels, Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly, 27 New Perspective Q. 15, (2010) at 1.

national asset. Protecting this infrastructure will be a national security priority."[24] Since the dawn of the Internet, the capabilities for good, including the distribution of immense knowledge and worldwide communication, have been greatly enhanced and utilized. Conversely, with the advent of this new technology came a unique array of Internet crime.

For millions of people around the world, much of their lives are online. Sensitive data such as email, credit card and bank accounts are all stored over the Internet. As such, modern day hackers have perfected the ways in which they can illegally access this information, putting our identities at risk. Although, as President Obama's remarks reveal, "cyber-crime" has now become so widespread and sophisticated that the threats it poses to U.S. national security can no longer go unnoticed.

In other words, national security concerns are necessarily raised when you take into account the target of the attack, as well as the intended effects. Conceptually, issues of national security arise when you distinguish between attacks against "vital" versus "non-vital targets."[25] Vital targets can be characterized as computer systems in relation to the five critical infrastructures –deemed vital because of the debilitating effect these attacks would have on the nation's economy and national defense.[26] The President's Commission on Critical Infrastructure Protection, (PCCIP), has identified the five critical infrastructures as; Information and Communication, Physical Distribution, Energy, Banking and Finance, and Vital Human Services.[27]

---

[24] Barack Obama, U.S. President Remarks on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/ the_press_ office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[25] Daniel M. Creekman, A helpless America? An examination of the legal options available to the United States in response to varying types of cyber-attacks from China, 17 Am. U. Int'l L. Rev. 641, 655 (2002).

[26] Id. at 655.

[27] Id. at 656.

Theoretically, many fear scenarios where a virus is implanted in the networks of financial institutions, scrambling financial records and stealing data. Likewise, it is conceivable that a sophisticated hacker could incapacitate the stock exchange or even set off a nuclear reactor.[28] As then Secretary of State Hillary Clinton noted on February 1, 2013, "over the last years [we have seen] an increase in not only hacking attempts on government institutions but also on nongovernmental ones…"[29] In this way, all aspects of the U.S. political and economic framework, from governmental agencies to financial institutions, as well as energy and power are at risk. However, in order to curtail these "cyber-criminals," it is first necessary to understand the threat presented and distinguish between "cyber-crimes," "cyber-attacks" and "cyber-warfare."

A. "Cyber-Attack/Warfare"

Judging by the remarks of President Obama and others, there is a mounting concern that the United States' cyber-infrastructure may be at risk. Many have stressed that threats to U.S. financial institutions, business and infrastructure are prime targets for hackers around the globe.[30] Yet, there are key distinguishing factors that separate "cyber-attacks" from "cyber-crime." Since the economy, power grid, and government agencies are so interconnected and depended upon by the general populace, the resulting debilitating effect to the United States' security would be immense. For example, a doomsday scenario where a hacker takes control of the New York Stock Exchange would threaten the U.S. economy, and thereby, raise national security concerns.[31]

[28] Oona A. Hathaway, et al. The Law of Cyber-Attack, Cal. L. Rev., 2012, at 1,7.
[29] Perlroth, *supra* note 2, at 1.
[30] Nakashima, *supra* note 1, at 1.
[31] Jeffrey Carr, Inside Cyber Warfare 176 (2010).

Some analysts have identified the resulting yearly cost of "cyber-attacks" to the U.S. economy as anywhere from $25 billion to $100 billion, or 0.1 to 0.5 percent of gross domestic product.[32] Likewise, bank analysts have posited that the collective costs of bolstering the cybersecurity of many financial institutions are in the hundreds of millions.[33] It is the enormity of the effect on the U.S. and its citizens as a whole that distinguishes "cyber-attacks" from mere "cyber-crimes."[34] Furthermore, a "cyber-attack" differs from a "cyber-crime" in that its principle objective is to not merely undermine the function of a computer network, but also, be politically motivated and/or affect national security.[35]

"Cyber-attacks" impact national security because they threaten to undermine the U.S. economy and the security of its citizens due to their potential far-reaching effects. On the other hand, national security concerns are clearly present when dealing with "cyber-warfare." According to the Joint Chiefs of Staff, "cyber-warfare" is defined as "information warfare" – operations designed to influence, disrupt, corrupt or usurp human and automated decision-making.[36] Furthermore, under this umbrella definition is included the subcategory of "network warfare."

In other words, "network warfare" is the employment of Computer Network Operations (CNO) with the intent of disrupting effective use of computers, information systems, and networks.[37] Admittedly, there is a fair amount of overlap between "cyber-attacks" and "cyber-warfare, but the distinction is apparent when you look at the effects of the attack. In fact, a "cyber-attack" may be indistinguishable from "cyber-warfare" in terms of the technology used in

---

[32] Nakashima, *supra* note 16, at 1.

[33] Ellen Nakashima & Danielle Douglas, More companies reporting cybersecurity incidents, Wash. Post, 1,2 Mar. 1, 2013, at 1.

[34] Hathaway, *supra* note 27, at 16.

[35] Id. at 18.

[36] Id. at 8.

[37] Id. at 8.

the attack or the particular type of attack. However, when the effects of the attack amount to the equivalent of an armed attack[38] or occur in the context of ongoing armed conflict, only then will the status of "cyber-attack" be elevated to "cyber-warfare."[39]

B. "Cyber-crime" and Tools of the Trade

On the other hand, while government actors and non-state actors alike may perpetrate "cyber-attacks/warfare", "cyber-crime" is solely restricted to criminal, non-state actors.[40] "Cyber-crimes" are generally divided into two basic types: 1) destructive or intrusive activity designed to destroy, alter or obtain the information contained on computers and/or networks and 2) crimes where computers are used to commit more traditional offenses.[41] Nevertheless, the tools and techniques employed by today's hackers are varied, much more complex, and go beyond simply attempting to steal information. Tools frequently utilized today include hacking, phishing, malware[42], Trojan horses[43] as well as distributed denial-of-service attacks, (DDOS).[44]

i. Hacking

There are many tools at the disposal of the everyday "cyber-criminal," but it is perhaps best to begin with hacking, one of the more widely recognized forms of "cyber-crime" and a moniker frequently associated with these type of actors. Generally, hacking can be described as the "surreptitious breaking into the computer, network, servers, or database of another person or

[38] When does a "cyber-attack" amount to an armed attack? Article 2(4) of the U.N. Charter – States may only use defensive armed force in response to a "cyber-attack" if the effects of the attack are equivalent to those of a conventional armed attack. Id. at 27.
[39] Id. at 18.
[40] Id. at 17.
[41] Decker, *supra* note 20, at 964.
[42] Malware is malicious software that causes computers or networks to do things that their owners or users would not want done. Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to do about it, 287 (2010).
[43] A Trojan horse is unauthorized software maliciously added to a program to allow unauthorized entry into a network or into the software program. Often after an initial entry, a cyber criminal or cyber warrior leaves behind a trapdoor to permit future access to be faster and easier. Id. at 289-298.
[44] Id. at 3.

organization."[45] Hacking can have far-reaching effects depending on the sophistication of the perpetrator, as well as the target the hacker intends to hit. Such attacks can infiltrate one's networks, bypass firewalls and securities, and steal valuable data.[46]

The utility of hacking allows "cyber-criminals" to not only obtain information, but also allows them to inflict damage.[47] For example, the hacker may release rogue programs such as viruses, malware, time/logic bombs[48], or even Trojan horses.[49] Overall, these tools allow a hacker to disable entire computer systems and servers. Today, U.S. industry and corporations are prime targets for hackers looking to steal trade secrets and intellectual property, (IP).[50] According to the Cyberspace Policy Review, issued by the White House in May 2009, analysts estimate that industry losses from IP theft as a result of hacking were as high as $1 trillion in 2008.[51]

ii. Phishing

Phishing, on the other hand, is a unique "cyber-crime" because it involves components of more traditional crimes such as, fraud or misrepresentations. According to the U.S. Department of Justice:

> [phishing is] the creation and use of e-mails and Web sites—designed to look like e-mails and Web sites of well-known legitimate business, financial institutions, and government

[45] Black's Law Dictionary (9th ed. 2009).
[46] Creekman, *supra* note 24, at 650.
[47] Id. at 650.
[48] A Logic bomb is a software application or series of instructions that cause system or network to shut down and/or to erase all data or software on the network. Richard A. Clarke *supra* note 41, at 287.
[49] Creekman, *supra* note 24, at 650.
[50] Alexander Melnitzky, Defending America against Chinese cyber espionage through the use of active defenses, 20 Cardozo J. Of Int'l & Comp. Law 537, 545 (2012).
[51] Id. at 545.

agencies—in order to deceive Internet users into disclosing their bank and financial information or other personal data such as usernames or passwords.[52]

Phishing is developing into a very sophisticated variant of "cyber-crime" because it necessarily involves two separate fraudulent acts: 1) assuming the identity of a legitimate financial institution or business; and 2) then fraudulently acquiring the personal data of the victim.[53] Thus, phishing is a potentially complex issue, because it not only involves multiple acts of fraud, but it also involves the additional hurdle of identifying the perpetrator. In the clearest sense, phishing is closely connected with spam, because spam provides the entry point into a personal computer and then an entire server or network. Spam is known as unsolicited email sent to a wide array of users –a concept many computer users can relate to.[54] Clicking on a fraudulent link sent through spam email is the first step for a "cyber-criminal" to infect your computer.

iii. Distributed denial-of-service attack (DDOS)

One final emerging method employed by "cyber-criminals" is a DDOS attack. A DDOS attack is designed to overwhelm the resources of a computer or server, thereby, denying access to legitimate users.[55] DDOS attacks are particularly powerful since they utilize more than one computer and inflict damage from a wider base of servers, thus further obscuring the identity of the assailant.[56] In comparison to hacking, which is generally aimed at attacking a single computer, DDOS attacks are directed at web sites in order to interrupt the stream of information

[52] Binational Working Group on Cross-Border Mass Mktg. Fraud, Report on Phishing 3 (2006), http://www.usdoj.gov/opa/report_on_phishing.pdf.
[53] Decker, *supra* note 20, at 976.
[54] Merriam-Webster Dictionary (2013).
[55] Decker, *supra* note 20, at 967.
[56] Id. at 967.

traveling to and from multiple computers, thus conceivably denying access to the computers, networks, and servers of an entire corporation or government organization.[57]

In these attacks, coordinated botnets[58] overwhelm servers by systematically visiting designated websites.[59] While DDOS attacks are frequently associated with non-state actors who attempt to cause no more than a nuisance and inconvenience, their utility in conducting more egregious and devastating attacks is on the rise.[60] For example, in 2007, Estonia suffered a DDOS attacks resulting in the incapacitation of emergency call lines to ambulance and fire stations –thereby presenting a real risk to civilians in need of emergency care.[61] Even so, hacking, phishing and DDOS attacks are merely some of the tools available today. Nevertheless, the question remains, in the event that you are attacked, what legal options are available?

II. Legal Options

According to Ronald Deibert, the Director of the University of Toronto's Citizen Lab, the difficulty in successfully prosecuting a hacker derives from the ever-expanding environment of cyberspace: "We have entered an age where anyone can participate in a cyber conflict from any point on earth, masking their location and their identity, yet causing serious disruption."[62] As a result, the legal recourse depends on key factors such as, whether the attacker is a private, non-state actor or working alongside a national military and/or at the direction of a government. This

[57] Id. at 968.
[58] A botnet is a network of computers that have been forced to operate on the commands of an unauthorized remote user, usually without the knowledge of their owner or operators. This network of "robot" computers is then used to commit attacks on other systems. A botnet usually has one or more controller computer, which are being directly employed by the operator behind the botnet to give orders to the secretly controlled devices. The computers on botnets re frequently referred to as "zombies." Botnets are used, among other purposes, to conduct floods of messages. Clarke *supra* note 41, at 282.
[59] Hathaway, *supra* note 27, at 22.
[60] Clarke *supra* note 41, at 13.
[61] Id. at 13.
[62] Interview by the Bulletin of the Atomic Scientists with Ronald Deibert, director of the University of Toronto's Citizen lab, (2011) at 1.

threshold question is essential in deciding which law applies –traditional criminal law, international law, etc.

A. Identification

Firstly, a state responding against a non-state actor/private citizen is generally a matter of law enforcement.[63] Therefore, if a U.S. citizen were accused of perpetrating a "cyber-crime," traditional criminal law would apply. For example, in U.S. v. Czubinski, the defendant was convicted of wire fraud and computer fraud for illegally browsing through the Internal Revenue Services', (IRS), databases.[64] On the other hand, if the private actor is not a citizen of the responding state, he/she may not be subject to the state's jurisdiction.[65] In the U.S., however, Congress oftentimes intends for certain criminal laws to apply extraterritorially; therefore, supplying a legitimate basis for jurisdiction over the foreign assailant. For example, the Hobbs Act is often utilized against foreign actors whose conduct, although outside the U.S., nonetheless affects commerce within U.S. boundaries.[66] Additionally, the responding state may still have to comply with applicable extradition agreements.

Meanwhile, while there are a several legal options available, successful prosecution of citizen-hackers is increasingly problematic due to in large part because of the difficulty in attributing blame. As a result of the inherent nature of anonymity over the Internet, it is understandably challenging to find the true source of an attack. This presents a particularly complex problem to prosecutors because the inability to determine identification gives the hacker the benefit of "plausible deniability."[67]

---

[63] Creekman, *supra* note 24, at 654.
[64] United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997)
[65] Creekman, *supra* note 24, at 654.
[66] 18 U.S.C.A. § 1951(a).
[67] Eric Talbot Jensen, Cyber warfare and precautions against the effects of attacks, 88 Tex. L. Rev. 1533, 1538 (2010).

Furthermore, certain attacks can be "crowd sourced" by governments or even arise out of acts of spontaneous participation –an almost mob-mentality over cyberspace.[68] For example, security experts hypothesized that the Russians, using this "crowd sourced" approach, may have orchestrated the 2007 Estonia "cyber-attacks" –however, the exact origins have yet to be verified.[69] Likewise, tracing the bread crumbs back to the hacker's Internet Protocol address, (IP address), presents one possible avenue, but even then a sophisticated hacker can utilize techniques to obscure the IP address or even hijack another's altogether –making identification close to impossible.[70] In this way, one of the central issues of cybersecurity is the difficulty in identifying the actor(s) behind the attack; differentiating between civilian and military backed attacks compounds this challenge even further.

B. Private Citizen Hacker

If an American citizen-hacker commits a "cyber-crime" in the United States against a private individual or corporation, laws ranging from traditional criminal laws of trespass, conspiracy, larceny, as well as statutes such as the Computer Fraud and Abuse Act, (CFAA), Hobbs Act, and wire fraud may apply.[71] Meanwhile, in the event that a private citizen hacks a governmental agency, the CFAA may be the prosecution's first line of recourse.[72] Accordingly, § 1030(a)(1) of the CFAA criminalizes whoever having knowingly accessed a computer without authorization and, thereby, obtained information deemed sensitive for reasons of national defense. [73]

---

[68] Bulletin of the Atomic Scientists, *supra* note 61, at 4.
[69] Id. at 4.
[70] Jensen, *supra* note 66, at 1538.
[71] Creekman, *supra* note 24, at 656.
[72] Id. at 658.
[73] 18 U.S.C.A. § 1030(a)(1).
a) Whoever--
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an

Conversely, attacks specifically directed at corporations or private entities are governed by § 1030(5)(A)-(C).[74] Therefore, depending on how the hacker transmits a virus or how he/she compromises and/or breaches a protected computer network, sections 1030(a)(5)(A)-(C) specifically look towards the intent of the perpetrator to inflict harm to a protected computer. Additionally, the Economic Espionage Act was enacted to handle theft of corporate insider information.[75] For example, in U.S. v. Aleynikov, the defendant, a former Goldman-Sachs employee, violated the Economic Espionage Act when he misappropriated computer source code used in high frequency financial trading.[76] The court found that he knowingly and intentionally

---

Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it

[74] 18 U.S.C. § 1030(a)(5)(A)-(C).

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss

[75] **(a) In general.**--Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--
(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) attempts to commit any offense described in any of paragraphs (1) through (3); or
(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.
(b) Organizations.--Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided. 18 U.S.C.A. § 1831.

[76] United States v. Aleynikov, 737 F. Supp. 2d 173 (S.D.N.Y. 2010)

copied and transmitted to his home computer, Goldman's proprietary source code with the intent to use the code for his own economic benefit, as well as that of his new employer.[77]

C. Foreign Hacker

While there exists a variety of criminal statues to utilize in prosecuting a citizen-hacker, when the attacker is based in a foreign nation, a certain amount of statutory construction is required. In Ivanov v. United States, the District Court of the District of Connecticut was asked to answer whether a defendant alleged to have hacked Online Information Bureau, Inc., (OIB), a Connecticut corporation, could be found guilty under the CFAA –even though he was physically located in Russia when he performed the act.[78]

The government alleged that Ivanov hacked into OIB's network, obtained passwords enabling him to control OIB's entire computer system, and then, through a series of unsolicited emails, demanded payment of $10,000 or else he would destroy their network.[79] While Ivanov argued that the CFAA was inapplicable in this case because he was in Russia and thus the court lacked subject matter jurisdiction, the court nevertheless found against him.[80] It is generally presumed that Congress intends for its acts to apply only within the boundaries of the U.S., however, this can be overcome with a showing of clear evidence of legislative intent for the act to apply extraterritorially.[81]

In this sense, the Ivanov court held that even though Ivanov was in Russia, the court did in fact have jurisdiction for two reasons: 1) because the intended and actual effects of Ivanov's actions occurred within the boundaries of the United States; and 2) Congress intended for the

---

[77] Id. at 177.
[78] United States v. Ivanov, 175 F.Supp.2d 367, 369 (2001).
[79] Id. at 369.
[80] Id. at 370.
[81] U.S. v. Gatlin, 216 F.3d 207, 211 (2d Cir.2000).

CFAA to apply extraterritorially.[82] The court further reasoned that even if the defendant's acts did not occur within American boundaries, Congress gave the district court jurisdiction under the Commerce Clause because the defendant's acts affected victims' commercial ventures in the interstate commerce within the U.S.[83]

Additionally, Congress in 1996 expressly amended the CFAA making several changes relevant to the issue of extraterritorial application.[84] Specifically, Congress amended the definition of "protected computer" so as to mean, "any computer which is used in interstate or foreign commerce or communication."[85] Interestingly, Congress had the foresight to anticipate "cyber-crime" as a future global problem and effectively extended the United States' jurisdictional reach into cyberspace. Yet, the effectiveness of applying the CFAA extraterritorially necessarily depends upon identifying the perpetrator, and in recent years, the U.S. has directed its attention towards China.

III. The Chinese Threat?

Evidenced by the prevalence of "cyber-crime" and the rise of "cyber-attacks" globally, the Internet presents a new frontier for modern day criminals who can now accomplish devastating acts affecting countless numbers of people without ever even leaving their homes. While anyone can read on the Internet and learn how to hack a computer, security experts worldwide have signaled that cyberspace is quickly becoming the new battlefield for modern day "cyber-warriors."[86] As Eugene Spafford, a computer scientist at Purdue University recently

[82] Ivanov, *supra* note 77, at 370. See. (United States v. Muench holding, if a defendant acts with intent to cause effects within the United States, it is reasonable to apply to persons outside the United States a statute that is not expressly extraterritorial in scope). See Also. (United States v. Steinberg holding, the government may punish a foreign-defendant as if he/she were present in the jurisdiction when the detrimental effects occurred).
[83] Stirone v. U.S., 361 U.S. 212, 215, 80 S.Ct. 270, 272, 4 L.Ed.2d 252 (1960).
[84] Id. at 78.
[85] Ivanov, *supra* note 77, at 373.
[86] James Fallows, Cyber Warriors, The Atlantic, March 2010 at 62.

remarked, "cyber crime is not conducted by some 15-year old kids experimenting with viruses…it is well-funded and pursued by…groups of professionals with deep financial…resources."[87]

Furthermore, recent events have shown that some professional hackers may not be acting on their own, but are working at the directive of governments.[88] Much has been made of the Chinese threat to the United States' cybersecurity, and while there may be some evidence to suggest that coordinated "cyber-attacks" have derived from China, it is clear that they are not the sole offenders.[89] The National Intelligence Estimate has identified Russia, Israel, and France as three of the world's leading nations with advanced cyber capabilities –not including the U.S.[90] Nevertheless, those in Washington, such as Mike Rogers, chairman of the House Intelligence Committee, continue to argue that "the Chinese government's direct role in cybertheft is rampant, and the problems have grown exponentially."[91]

While China's name has certainly come up in recent times, predominantly since events such as the hacking of Google, attacks on homeland security, attacks on defense contractors, and most recently, the New York Times, the United States' vulnerabilities to "cyber-attacks" cannot simply be pinned upon a more aggressive China. Rather, the U.S. government, and Congress specifically, have been slow to react to the emerging reality that there is a new battlefield emerging, and it's online.

A. A Concerted Campaign of Cyber-Espionage?

[87] Id. at 62.
[88] Id. at 62.
[89] Nakashima, *supra* note 16, at 1.
[90] Id. at 1.
[91] Craig Timberg & Ellen Nakashima, Chinese cyberspies have hacked most Washington institutions, experts say, Wash. Post, February 20, 2013, at 1.

When people think of possible Chinese "cyber-crimes" against the U.S., they often mention the threats to corporate entities because attacks like those against Google or the New York Times are more personally relevant. Meanwhile, events as of late suggest that there are three specific areas that are most at risk: 1) U.S. military; 2) corporate entities; and 3) political news media.

In fact, according to Mandiant, a U.S. security firm, the Chinese military has been linked to the hacking of over 140 U.S. and other foreign corporations and entities.[92] After compiling seven years of research, Mandiant traced these attacks back to a single group identified as, Advanced Persistent Threat 1, (APT1).[93] Mandiant argues that APT1 is a Chinese military unit located within the second Bureau of the People's Liberation Army General Staff Department's Third Department, code named, "Unit 61398."[94]Not surprisingly, China has steadfastly denied such allegations.

Mandiant's research suggests that since 2006:

> 141 companies spanning 20 major industries [have been hacked, and]…of those victims, 87 percent are headquartered in countries where English is the native language…115 of them are located in the United States, two in Canada and five in Britain. Of the 19 others, all but two operate in English.[95]

Mandiant contends that what they have uncovered is what many analysts have long presumed; however, their research stands out from the rest because they have identified the IP addresses used in recent "cyber-attacks" on U.S. corporate entities.[96] According to Project 2049 Institute, an American think-tank, "Unit 61398" is approximately the size of the National

[92] Wan & Nakashima, *supra* note 6, at 1.
[93] Id. at 1.
[94] Id. at 1.
[95] Id. at 1.
[96] Id. at 1.

Security Agency, (NSA) –strongly suggesting that the Chinese Party has been playing a guiding role in "cyber-attacks."[97] Additionally, this report argues that the unit's 12-story building, equipped with special fibre-optic communications, is staffed by hundreds of specially trained individuals in network security analysis, digital processing, covert communications, and English linguistics.[98]

In fairness, as Hong Lei, China's Foreign Ministry spokesman pointed out, "hacking attacks are transnational and anonymous…determining their origins is extremely difficult."[99] While this is undoubtedly true, Richard Beijtlich, Mandiant's Chief Security Officer, maintains that the veracity of their investigation lies in their close cooperation with the U.S. intelligence agencies –without whose authority, these findings would never have been published.[100]

While it is certainly true that it is almost impossible to pinpoint the exact origin of a "cyber-attack," given the anonymity of the Internet, there may be some telltale indicators suggesting China may be responsible. According to analysts at CrowdStrike, a cybersecurity firm, the indiscriminate tactics employed by the Chinese make it relatively easy to track.[101] In other words, China's brazenness and carelessness in conducting these "cyber-attacks" leave little doubt in the minds of many analysts.[102] For example, China will hack an organization and then reside there for five or six years; or employ an attack that sends data back to Chinese websites.[103] Yet, the attacks persist.

i. Attacks on the Military

[97] Masters of the cyber-universe: China's state-sponsored hackers are ubiquitous—and totally unabashed, The Economist, Apr. 6, 2013, at 1.
[98] Hello, Unit 61398, The Economist, Feb. 19, 2013, at 1.
[99] Wan & Nakashima, *supra* note 6, at 2.
[100] Id. at 2.
[101] The Economist, *supra* note 96, at 1.
[102] Id. at 1.
[103] Id. at 1.

As the Chinese continue to deny any and all accusations, security analysts and those in Washington continue to stress that the U.S. is at risk. Principally, of chief national security concern are attacks against information technology, (military and aerospace technology, satellites and telecommunications, scientific research and consulting).[104] Mike McConnell, former director of National Intelligence, argues that the Chinese realize that the United States' strength lies in its military –a force it knows it does not have the resources to compete with.[105] Conversely, China also realizes that the "strategic vulnerability of the United States is its soft cyber underbelly…[and he believes] China seeks to own that space."[106]

Therefore, McConnell contends that China seeks to exploit "our systems for information advantage—looking for the characteristics of a weapons system by a defense contractor or academic research on plasma physics."[107] For example, in 2008, the cyber-espionage ring termed, "Titan Rain," sparked U.S. national security concerns when it stole information from military labs, NASA, as well as the World Bank.[108] "Titan Rain" further extended its reach when it also hit the Department of Homeland Security, penetrating the department's network by programs that sent massive amounts of information to Chinese websites.[109] Shawn Carpenter, an analyst at Sandia National Laboratories originally brought the attack to light by tracing the attack back to a team of government-sponsored researchers in Guangdong Province.[110] Also in 2008,

[104] Nakashima, *supra* note 16, at 1.
[105] Gardels, *supra* note 22, at 16.
[106] Id. at 15.
[107] Id. at 15.
[108] Josh Rogin, The Top 10 Chinese Cyber Attacks (That We Know of), Foreign Pol'y (Jan. 22, 2010, 8:57 PM), http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of#.
[109] Melnitzky, *supra* note 49, at 544.
[110] Rogin, *supra* note 108, at 1.

Chinese hackers supposedly stole data on F-35 fighter planes being developed for the U.S. military by Lockheed Martin.[111]

ii. Attacks on Corporate Entities

Nevertheless, recent events have shown that if China is in fact infiltrating the United States' cybersecurity, it appears as though obtaining information may be the higher priority.[112] China is a nation of manufacturing prowess but with little innovations of its own.[113] McAfee's vice president of threat research, Dmitri Alperovitch, remarking on stolen data reported by U.S. companies, maintains that stolen IP and trade secrets are particularly concerning.[114] "If even a fraction of it is used to build better competing products or beat a competitor at a key negotiation, (due to having stolen the other team's playbook)…[it] represents a massive economic threat."[115]

One of the more infamous hackings in recent memory occurred in 2010 when Google claimed the Chinese had attacked its networks.[116] According to a leaked U.S. intelligence cable, China was becoming suspicious of Google and worried that it threatened to challenge official censorship of the Internet by becoming more appealing to Chinese net users.[117] In this way, it is believed that the government feared that the U.S. and Google were working in concert to undermine Chinese governmental control of the Internet.[118] In the aftermath of the incident, China summarily denied everything.[119] Nevertheless, Google chief executive, Eric Schmidt, did not restrain himself when he proclaimed, "China is the world's most sophisticated and prolific

---

[111] Siobhan Gorman et al., Computer Spies Breach Fighter-jet Project, Wall St. J., Apr. 21, 2009, http://online.wsj.com/article/NA_WSJ_PUB:SB124027491029837401.html.
[112] Gardels, *supra* note 22, at 15.
[113] Kenneth Lieberthal, The United States and China have enjoyed the fruits of Beijing's WTO entry, but insufficient change in China's political economy may spell trouble for the future, China Business Rev. 53,56, (2006).
[114] China chief suspect in biggest-ever, most audacious international cyber pilferage, Tibetan Rev. (Sept. 2011).
[115] Id. at 1.
[116] China leadership orchestrated Google hacking, BBC News, (Dec. 4, 2010, 6:40 AM), http://www.bbc.co.uk/news/world-asia-pacific-11920616.
[117] Id. at 1.
[118] Id. at 1.
[119] Id. at 1.

hacker…it's fair to say we're already living in an age of state-led cyberwar, even if most of us aren't aware of it."[120]

iii. Attacks on News Media

Lastly, recent reports suggest that the Chinese may be looking beyond stealing corporate trade secrets. Over the years, China's government has been in transition in terms of its laws and economy –yearning for parity among the other world powers.[121] As a result, Dan Blumenthal, director of Asian studies at the American Enterprise Institute, posits that China has adjusted its gaze towards news media, seeking out journalists with access to political actors.[122] In this way, China wants to understand how Washington works.[123] Furthermore, in February of 2013, when the New York Times, Washington Post and other news organizations reported being hacked, security experts said that the Chinese were motivated by a desire to closely monitor the way China's politics are handled in the U.S.[124]

Likewise, when U.S. diplomats were investigating the Google incident, they cited a Chinese source arguing that the root of the problem stemmed from an unnamed member of the politburo standing committee who realized, after searching his name in Google, that there are critical stories being written about him.[125] A report by Mandiant suggests that Chinese hackers have stolen emails, contacts and files of many U.S. journalists, creating a short list of names for repeated attacks in the future.[126]

More specifically, China is targeting those who had written about Chinese leaders, politics and legal issues, as well as articles about Chinese telecommunications giants Huawei and

---

[120] Nakashima, *supra* note 16, at 1.
[121] Wang Yong, China in the WTO: A Chinese View, China Business Rev. 43, 43, (2006).
[122] Craig Timberg & Ellen Nakashima, Chinese cyberspies have hacked most Washington institutions, experts say, Wash. Post, February 20, 2013 at 1.
[123] Id. at 1.
[124] Perlroth, *supra* note 2, at 1.
[125] BBC News, *supra* note 115 at 1.
[126] Perlroth, *supra* note 2, at 1.

ZTE.[127] In this way, China's chief concern may be surveillance and spying. Andrew Nathan, a professor at Columbia University maintains that China, as a nation predicated upon control, finds utility in its reconnaissance as a result of paranoia setting in and the need to monitor everything.[128]

Whether or not China, the governmental body, is responsible for hacking U.S. news organizations because it is paranoid about the U.S. mishandling Chinese politics; whether or not the government is responsible for coordinating attacks on U.S. military organizations for information technology, or even if non-state actors are attacking corporations for IP, the attacks are happening. Perhaps it is fair for China to continue to deny any and all accusations, considering conclusive proof that it is behind these "cyber-attacks" is lacking. Nevertheless, U.S. corporations continue to be at risk, the U.S. military departments are bolstering their cybersecurity, and the administration is issuing stern warnings –regardless of the fact that it is possible that non-state actors may be committing these acts, they are occurring under China's watch. China is not doing anything about it and yet, reaping the rewards.[129]

IV. U.S. Cyber Policy and Recommendations Moving Forward

> At the beginning of the era of strategic nuclear war capability, the U.S. deployed thousands of air defense fighter aircraft and grounded missiles to defend the population and the industrial base…At the beginning of the age of cyber war, the U.S. government is telling the population and industry to defend themselves…can you imagine if in 1958 the Pentagon told U.S. Steel and General Motors to go buy their own Nike missiles to protect themselves?[130]

---

[127] Id. at 1.
[128] Timberg & Nakashima, *supra* note 121, at 1.
[129] Nakashima, *supra* note 1, at 1.
[130] Clarke & Knake, *supra* note 41, at 144.

Nonetheless, the question remains, whose job is it to defend the United States' infrastructure and industry in the event of a massive "cyber-attack?"[131] It is no secret that the United States is a nation with military superiority. Likewise, the U.S. may very well possess the most sophisticated offensive cyber capabilities. While this is true, a first rate offense is of no use if you are the one always on the defensive, and the United States' cyber defenses pale in comparison.[132] More specifically, in terms of legislation, the U.S. is deficient. Yet, in a stroke of poetic irony, recent attacks attributed to the Chinese, may be the wake-up call the U.S. needed.

For the past few years, cybersecurity legislation, though limited, has been coming across the senate floor. Most recently, the Cybersecurity Act of 2012, introduced by Sen. Joe Lieberman and Sen. Susan Collins, was a bill that appeared to gather many in government around a central concern over cybersecurity. Although it failed, it was reintroduced in February of this year and there are encouraging signs that similar bills will follow.

Nevertheless, when Congress finally approves a bill, those pieces of legislation must increase the role of corporate transparency, promote the education of cyber-related offenses, and further the public-private cooperative to establish active defenses against potential "cyber-attacks." Therefore, this paper will argue that, in light of the backdrop of on-going Chinese "cyber-espionage" of government agencies, as well as the pilferage of corporate trade secrets, Congress must react and pass new legislation.

A. U.S. Cyber policy

[131] Id. at 144.
[132] Id. at 145.

Since the days of the Clinton Administration, the U.S. Cyber Policy has centered around a public-private partnership.[133] In 2000, President Clinton established the National Information Systems Protections Plan declaring that the United States' cybersecurity is dependent upon the private sector and the public sector working together.[134] Every subsequent president has essentially reiterated this plan –Bush in 2003 with his National Strategy to Secure Cyberspace and Obama in 2008 with his Cyberspace Policy Review.[135]

In fact, President Obama issued an executive order on February 12, 2013 to improve critical infrastructure cybersecurity calling upon more public-private cooperation.[136] With this order, President Obama is urging corporate entities to adhere to a voluntary set of standards in order to facilitate the communication between American industry and government about detecting cyber threats.[137] This enhanced transparency is a critical step according to Jacob Olcott, a cybersecurity expert with Good Harbor Security Risk Management, because the mutual sharing of detected network intrusions will expose weaknesses within America's cyber-infrastructure.[138]

While the executive branch has been calling upon greater recognition of the growing threat to U.S. cybersecurity, the U.S. military has slowly evolved to meet these emerging challenges as well. In 2002, the Pentagon delegated centralized control of U.S. "cyber-war" operations to Strategic Command, (STRATCOM), a unit in charge of missile defense, space operations, as well as intelligence and surveillance.[139] However, cyber capabilities were low on

---

[133] Melnitzky, *supra* note 47, at 546.
[134] White House. National Plan for Information Systems Protections version 1.0: An Invitation to a Dialogue (2000), http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf
[135] Id. at iv.
[136] Exec. Order No. 13636, 3 C.F.R. (Feb. 12, 2013).
[137] Nakashima, *supra* note 1, at 1.
[138] Nakashima & Douglas, *supra* note 13, at 1.
[139] Melnitzky, *supra* note 49, at 549.

its list of priorities, and so it was the Air Force that truly took the initiative to become the leader in "cyber-war," until the formation of Cyber Command in 2010."[140]

In 2010, the NSA unified all of the existing military cyber activities conducted by the military, navy and other departments under a single command headed by Army Gen. Keith Alexander.[141] Initially, it was designed to bolster the security of the Pentagon but is gradually extending its reach to other branches of government.[142] Although, as time has gone by, Cyber Command helped create cyber components within the Army, Navy, Air Force and Marine Corps, and has joined forces with cyber professionals to protect the networks of the Pentagon, as well as defense contractors.[143] Nonetheless, while a greater emphasis on cybersecurity, spearheaded by the administration and military, is a step in the right direction, critics of Cyber Command, such as Rep. Mac Thornberry maintain, "we are still playing catch-up, and part of that is Congress' responsibility."[144]

B. The Legislature and Legal Recommendations

While the Executive branch and the divisions of the military have signaled that cybersecurity is now a top priority, Congress in contrast, has been relatively slow to react.[145] While President Obama's executive order serves as a catalyst for all branches of the government to increase the role of cybersecurity in future decision-making, it is only a small step. For example, Rep. McCaul has maintained that Congress must assume the responsibility and draft cybersecurity legislation because an executive order cannot grant new authorities or provide liability protection for corporations.[146]

---

[140] Id. at 549.
[141] Year-old Cyber Command has more growing to do, Gannett 1, (Aug. 8, 2011).
[142] Id. at 1.
[143] Id. at 1.
[144] Id. at 1.
[145] Martinez, *supra* note 21, at 1.
[146] Id. at 1.

Nevertheless, there has been some activity in Congress in recent years. For example, the Cybersecurity Act introduced by Sen. Lieberman and Sen. Collins in 2012, was a promising bill because it seemed to address the pressing issues presented by cyber-threats and also achieve a good amount of bipartisan support.[147] Yet, to the surprise of many, Congress did not agree.[148] Despite its bipartisan backing, argues House Homeland Security Committee Chairman McCaul, many saw the bill as an attempt to over-regulate the private sector and so, presented civil liberties and privacy concerns that many could not overlook.[149]

The major obstacle facing the passage of a comprehensive cybersecurity bill stems from the fact that computers have become so ubiquitous in our everyday lives "that they cross every sector of the economy—and nearly every congressional committee's turf."[150] In 2010, the Senate Committee on Commerce, Science and Technology introduced the Rockefeller-Snow Cybersecurity Act.[151] Like Sen. Lieberman and Sen. Collins' bill, opponents feared over-regulation in the forms of attacks on corporate privacy, trade secrets, etc.[152] However, proponents of the Rockefellar-Snow Act argued that the bill was minimally regulatory and in fact, created incentives for businesses that would allow them to act in accord with the government to expose and remedy "cyber-attacks."[153]

In a similar way, the Intelligence Committee's Cyber Intelligence Sharing and Protection Act, (CISPA), was attacked by various civil liberties groups as an assault on privacy.[154] On the other hand, companies that have recently succumbed to "cyber-attacks" are presently endorsing

---

[147] Erik Kain, Does the Cybersecurity Act of 2012 mark the beginning of the war on cyber-terrorism?, Forbes, 1 (Feb. 2, 2012), at 1.
[148] Finan, *supra* note 14, at 1.
[149] Id. at 1.
[150] T.S., Cyber-Security in Congress, Economist Blog (Aug. 3, 2010, 2:15 PM), http://www.economist.com/blogs/democracyinamerica/2010/08/cyber-security.
[151] Melnitzky, *supra* note 49, at 551.
[152] Id. at 551.
[153] Id. at 552.
[154] Martinez, *supra* note 21, at 1.

likeminded legislation –entities like, Facebook, AT&T, and IBM.[155] Conceivably, lawmakers could combine the best of the 2012 Act with CISPA to create a program in which companies would share information about malicious source code and other data with the intelligence communities, and in the process, create strong incentives for corporation to join in.[156]

The White House's official cybersecurity policy advocates a program designed to reduce the threat globally—"by working with allies on international norms of acceptable behavior in cyberspace, strengthening law enforcement capabilities against cybercrime, and deterring potential adversaries from taking advantage of our remaining vulnerabilities."[157] Addressing the global threat and working with allies is certainly a utilitarian approach to formulating a certain standard of cybersecurity conduct and ethics. However, Congress has the power to create legislation that could put in place certain laws and procedures that can have practical and immediate effects on U.S. cybersecurity at home. Fortunately, this appears to be the trend, and there is bipartisan support. Even so, what can Congress do to pass a comprehensive bill that can adequately address these issues?

i. Corporate Transparency

One of the keys to any forthcoming legislation is ensuring the private sector that it will not be overly regulatory –yet, there are signs that corporate America and Washington are coming together. "Alongside terrorism, cybersecurity is perhaps the number one threat facing [the] nation today," commented Sen. Feinstein.[158] In this way, the ubiquity of "cyber-attacks" against government agencies has gotten many politicians up in arms; however, so too have the attacks against U.S. industry. Corporations such as eBay, Chesapeake Energy and AT&T have admitted

[155] Id. at 1.
[156] Id. at 1.
[157] White House Cybersecurity (2013). http://www.whitehouse.gov/cybersecurity
[158] Kain, *supra* note 144, at 1.

that they have recently suffered network intrusions.[159] Likewise, Paul Smocer, president of BITS, a financial services trade organization, correctly proclaims "it's almost naïve for most large companies in the critical infrastructure sector to say that they aren't subject to attack."[160]

In fact, since President Obama's executive order, asking for greater disclosure of network intrusion incurred by corporations, at least nineteen financial institutions have admitted to recent "cyber-attacks" – an encouraging sign of growing openness between the public and private spheres.[161] For example, Fifth Third Bank of Cincinnati recently disclosed that it endured a DDOS attack last year and as Debra DeCourcy, a bank spokeswoman asserted, "if there is something else positive that can be gained from that, it's all the better." [162]

A bill that further fosters this openness between corporate America and the government is key in isolating cybersecurity flaws, shoring up defenses, as well as identifying those perpetrators behind the act. Similarly, a "cyber-attack" on a major U.S. corporation is inextricably tied to the fate of the U.S. economy as a whole. Therefore, there is a benefit in an additional measure incorporating certain Securities and Exchange Commission, (SEC), guidelines encouraging greater corporate disclosure of "cyber-attacks."[163]

In other words, in the way that the Dodd-Frank Wall Street Reform and Consumer Protection Act imposed greater disclosure of material information included in corporate prospectus; the SEC could enact similar schemes concerning cybersecurity.[164] Therefore, a typical investor who would judge the risk factors in investing in a corporation based on its profit margins and/or growing market could benefit from a list of risk factors concerning company X's

---

[159] Nakashima & Douglas, *supra* note 13, at 1.
[160] Id. at 1.
[161] Id. at 1.
[162] Id. at 1.
[163] Ellen Nakashima and David S. Hilzenrath, Cybersecurity: SEC outlines requirement that companies report cyber theft and attack, Wash. Post, 1,1, Oct. 14, 2011, at 1.
[164] Dodd-Frank Wall Street Reform and Consumer Protection Act. http://www.sec.gov/about/laws/wallstreetreform-cpa.pdf

cybersecurity. The prospectus could include a companies' history of "cyber-attacks," their current level of security, etc. –information that would tell an investor whether or not it is a wise investment.

Even so, in order to bring industry into the fold, legislators must draft a bill in such a way as to not over-regulate or compromise privacy. Therefore, in the minds of corporate leaders, any bill that is overly obtrusive, to the extent that it may affect profits, would present a problem for the fate of future legislation. In other words, a future bill must strike the balance between safeguarding against "cyber-attacks" and protecting privacy. Generally, corporations are reluctant to advertise that their cybersecurity has been compromised because of their concern on how it will appear to its investors and/or adversely affect its profit margins.[165] Likewise, as one bank official put it, "every time we give detail on what we know about the threats, we're sharing that with those who might be looking to target us."[166]

Therefore, a carefully drafted bill should include incentives, such as liability protections so that a corporation would not feel reluctant to share information about past attacks and thus, help identify past and possibly on-going threats. Additionally, preferable tax treatment or exemptions can bring more to the table –thereby ensuring that corporate expenditure in cybersecurity is worthwhile.[167] Furthermore, with the proposed SEC regulations in mind, certain statutory penalties for non-compliance can also be a motivating factor for corporations –in turn persuading their lobbyists and/or lawmakers to approve cybersecurity legislation.

ii. Cyber-education

While corporate transparency and openness is a crucial step to a greater understanding of the threats to the U.S. and industry, education is similarly a fundamental factor. In this way,

[165] Nakashima, *supra* note 1, at 1.
[166] Nakashima & Douglas, *supra* note 13, at 1.
[167] Id. at 1.

strides have in fact been made in the area of cyber-capabilities education with the Comprehensive National Cybersecurity Initiative, (CNCI), and in 2010, the National Initiative for Cybersecurity Education, (NICE).[168] Likewise, in a legal sense, the Justice Department has taken it upon itself and begun training hundreds of prosecutors to combat and prosecute "cyber-espionage" and other related cyber crimes to meet this growing threat to national security.[169] This new initiative seeks to train and develop prosecutors to identify and aptly respond to cyber related crimes.[170]

Assistant Attorney General for National Security, Lisa Monaco, describes this as a realignment of U.S. counterterrorism efforts –"just as we [did]…after 9/11, we are realigning our cyber effort to meet this challenge." [171] Therefore, teams of lawyers within the justice department's new national security division, (NSD), will work with both the military and corporations to develop protocols for the intelligence community in how to deal with private companies fallen victim of "cyber-attacks."[172] More specifically, this division will focus on how to construct possible prosecutions within issues revolving around information sharing, privacy and civil liberties.[173] As a first measure, at least one prosecutor in each of the U.S. attorney's offices around the U.S. will be specifically assigned this post.[174]

Nonetheless, while training a new generation of U.S. attorneys is a forward-looking and worthwhile step in combating "cyber-crime" and "cyber-attacks" in America and beyond, a clearer understanding of network security is also warranted across the board. More specifically,

---

[168] White House, National Initiatives for Cybersecurity Education (2010), http://www.whitehouse.gov/sites/default/files/rss_viewer/cybersecurity_niceeducation.pdf (This document describes the four-track program established and the government agencies responsible for them.)
[169] Sari Horwitz, Justice Department trains prosecutors to combat cyber espionage, Wash. Post, 1 (Jul. 25, 2012), at 1.
[170] Id. at 1.
[171] Id. at 2.
[172] Id.
[173] Id. at 1.
[174] Id.

today we are seeing a greater frequency of attacks on corporate entities, news media organizations, research institution, and law firms. In this way, CEOs, board members, directors, and even partners in law firms must educate themselves and their employees about the present dangers and what to do in the event of an attack.

For example, information packages can be disseminated to law firms and/or boardrooms containing vital information on what to do when you suspect a cyber-intrusion, what warning signs are there to look out for, information on avoiding viruses, spam and checking emails, and what legal remedies are available in the event of an attack.[175] Practical and simple measures such as these can mean the difference between safeguarding vital information from a "cyber-attack," and losing it all. Once again, mass appeal for measures such as these can be garnered through added incentives and tax exemptions. In other words, having corporations expend the added expense must be assured that these preventive actions are not in vain. Likewise, in light of the fact that smaller organizations like law firms and research centers of universities also experience "cyber-attacks," a tax exemption incentive is economically appealing.

iii. Private-Public Cooperation to form Active Defenses

The areas of education and corporate transparency are two practical ways in which future cybersecurity legislation can effectively curb the prevalent threat of corporate "cyber-attacks." Yet, protecting every computer in the U.S. is an insurmountable obstacle, however, given the interconnected nature of the Internet across the country, protecting the U.S. cyber-infrastructure on a macro scale may by extension protect everyone else. A strategy of active defensive measures is more practical than simply having the greatest offensive capabilities and this can be

[175] Vince Farhat et al., Cyber Attacks: Prevention and Proactive Responses, Practical Law Company, (2011). http://us.practicallaw.com/3-511-5848.

accomplished by focusing on key sectors.[176] For example, in the U.S. there are many Internet Service Providers, (ISP), however, AT&T, Verizon, and Sprint are some of the handful of major providers in the nation. Over 90% of the Internet traffic in the U.S. moves over these "Tier 1" providers –including military and government agency buildings.[177]

Therefore, even though this is a plan that is not necessarily geared towards protecting everyone, you can effectively safeguard the majority of U.S. cyberspace if you shield "Tier 1" providers –in other words, the "backbone" of the Internet in America.[178] For example, if a hacker intended to infiltrate the network of a fortune 500 company, he/she would have to connect to the Internet first.[179] Thus, the hacker would have to confront this first wave of defenses before ever setting sight on the intended corporate target.[180] Therefore, once Verizon or other "Tier 1" providers detect an intruder, it can inform law enforcement and/or the FBI and thus provide all pertinent information about the hacker, extent of the damage, vulnerabilities, and possibly its origin.

Furthermore, this sort of scheme is similarly applicable to large energy suppliers. In a worst-case scenario, a hacker could infiltrate the securities of an energy company and effectively turn off the electricity of the entire east coast of the U.S. –cutting off the power to vital government buildings, hospitals, and/or air traffic control systems. Therefore, it seems logical that the government and these energy suppliers work in conjunction with Internet providers and expand the network of first wave defenses. As in the case of incentivizing corporations to approve and adopt these new proposals, here, Congress must formulate a way to incentivize

[176] Clarke & Knake, *supra* note 41, at 160.
[177] Id. at 160.
[178] Id. at 160-161.
[179] Id. at 161.
[180] Id. at 161.

Internet and energy giants. Therefore, similar tactics, such as penalties for non-compliance, favorable tax treatment and/or write-offs are practical measures that can be incorporated.

Likewise, a fair amount of research and development is necessary to accomplish this planned task of active defenses. In this way, it is foreseeable that the government and military agencies could work in tandem with Internet providers and energy suppliers to development the necessary technology this proposal envisions. That being said, when discussing Internet providers and the government teaming up, and scrutinizing users who travel in and out of cyberspace, valid privacy concerns are raised. Therefore, it is crucial that future cybersecurity legislation strikes a balance between information sharing and protection, and user privacy. Although, that may a questioned better suited for law enforcement and the FBI to answer.

IV. Conclusion

For the sake of national security, Congress must react to the emergence of "cyber attacks" and "cyber-espionage." While many are charging that the Chinese are intent on taking over cyberspace and, thereby threatening U.S. security, the reality is that the U.S. is vulnerable to these attacks, and they may be coming from anywhere. Nevertheless, the recent attacks identified as coming from China are illustrative of the problems the U.S. faces. In other words, people may agree that China is stealing trade secrets, but so is Russia or Iran. To that end, Congress must act and draft legislation that effectively shields the U.S. from similar attacks.

This paper advocates a plan that proposes three practical and effective ways to accomplish increased cybersecurity and greater information sharing to curtail future "cyber-attacks." Firstly, a bill must call upon more corporate transparency. Secondly, education about "cyber-attacks," "cyber-crimes" and related cyber offenses is required across the board. In other words, corporate directors, managers and employers must educate themselves, as well as their employees about

the threats to look out for, and what to do in the event of an attack. Beyond that, increased education within the legal profession is a forward-looking endeavor that will prepare the government to seek out and prosecute hackers.

Lastly, the U.S. government, Internet providers and energy suppliers must come together to establish active defensive measures. When an intruder is suspected, immediate action to identify and neutralize the threat is imperative. Overall, it is Congress' responsibility to enact legislation that can effectively safeguard the nation from future "cyber-attacks." In the face of such prolific and on-going suspicion of Chinese network intrusion, affecting government, industry and defense alike, Congress must intervene. The utility of the Internet as a tool to commit criminal acts, acts of war, or even acts of terror is the reality that all nations face. Given the proliferation of the Internet and given that evidence documenting how vulnerable the United States' cybersecurity is, there is no better time to act.