2018

Critical Infrastructure, Cybersecurity, and Market Failure

John J. Chung
Roger Williams University School of Law, jchung@rwu.edu

JOHN J. CHUNG*

Critical Infrastructure, Cybersecurity, and Market Failure

When most people think of cybersecurity and cyberattacks, their attention probably turns to privacy violations and theft of personal information—invasions of personal security. This is natural given well-publicized incidents in recent years, including the data breaches of personal information from customers of national retail businesses such as Target and Home Depot, as well as large banks.[1] These are harmful incidents, to be sure, and incidents like these affect millions of people. However, there are more serious threats with the potential to cause damage beyond the individual level. Without a doubt, invasions of privacy, including breaches of personal health and financial records, are serious matters. Nonetheless, there are dangers with the potential to cause great harm to national and societal security. Cyberattacks involve more than theft of information; they can damage or destroy property, which in turn can lead to loss of life (perhaps even large-scale loss of life). This is especially true for

* Professor, Roger Williams University School of Law; B.A., Washington University (St. Louis); J.D., Harvard Law School.

[1] *See* Kristin N. Johnson, *Managing Cyber Risks*, 50 GA. L. REV. 547, 550–52 (2016).

attacks on systems that are designated as critical infrastructure.[2] This Article addresses the issue of cybersecurity and threats to critical infrastructure from individuals, nation-states, and/or groups of individuals (working on behalf of or independently of nation-states).

To understand the threat, several recent events deserve attention. On December 23, 2015, a control center in western Ukraine lost control of the electrical power grid for that region.[3] A cyberattack shut down the substations despite the efforts of the operators to regain control of their computer network.[4] One operator's computer logged him out of the system and prevented him from regaining entry.[5] The computer then proceeded to shut down about thirty substations.[6] The attackers struck two other power distribution centers at the same time and disabled backup power supplies.[7] More than 230,000 people lost power in the dead of winter. This was the first confirmed cyberattack that shut down a power grid.[8] According to the investigation following the attack, the attack was planned over many months.[9] The hackers conducted reconnaissance to study the networks and access operator credentials, and then they launched a synchronized assault.[10] One of the investigators (a former cyberwarfare operations officer in the U.S. Air Force) noted the sophistication in logistics, planning, and operation.[11] Although the identity of the cyberattackers is uncertain, Ukraine blamed Russia for the attack.[12] What should cause concern

---

[2] The language used to describe these threats is not particularly helpful in encouraging an examination of the distinction between personal threats versus national/societal threats. The terms "cybersecurity" and "cyberattacks" are used loosely and describe a wide range of activity (from annoying to criminal, committed by actors ranging from lone hackers to nation-states). "Cybersecurity is also sometimes conflated inappropriately in public discussion with other concepts such as privacy, information sharing, intelligence gathering, and surveillance." ERIC A. FISCHER, CONG. RESEARCH SERV., R43831, CYBERSECURITY ISSUES AND CHALLENGES: IN BRIEF 1 (2016).

[3] Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.* Russia is also suspected of conducting a cyberattack on Estonia's critical infrastructure in 2007. The attack shut down Estonia's banking system, telephone connections, and television networks. *See* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U.L. REV. 1503, 1504 (2013).

for Americans is that the Ukrainian cybercontrol systems were thought to be stronger and more secure than the systems in place for many power grids in the United States.

It appears that the attack on the Ukrainian power grid was not intended to result in permanent damage. It may have been conducted to send a message. If that was the case, Ukraine was fortunate.

> A cyber-attack on the power grid would be truly catastrophic. The industrial control, or SCADA, systems used by power plants and other utilities are increasingly connected to the Internet. Hackers could exploit this connectivity to disrupt power generation and leave tens of millions of people in the dark for months. They could even destroy key system components like turbines.[13]

The attack on the Ukrainian power grid may have been exceptional only insofar as its effectiveness. There are reports that electric utilities are probed thousands of times each month by hackers and that nation-states designed plans for attacking the power grids of other countries.[14]

In 2016, another group of hackers stole $81 million from the Bangladesh Central Bank.[15] There is speculation that the hackers breached the Bank's network, which was made possible by a lack of firewall protection.[16] The money was transferred into the accounts of casinos in the Philippines; from there, the money disappeared.[17] A central bank is a nation-state's bank. This was a theft from the

---

[13] Sales, *supra* note 12, at 1514. A report from the Congressional Research Service states,

> attacks on *industrial control systems* can result in the destruction or disruption of the equipment they control, such as generators, pumps, and centrifuges. Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens.

FISCHER, *supra* note 2, at 2–3.

[14] *See* Scott J. Shackelford et al., *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995, 2005–06 (2016) [hereinafter Shackelford et al., *Sustainable Cybersecurity*]. The *New York Times* recently reported that North Korea may acquire the capability to launch a cyberattack on the United States' power grid. *See* David E. Sanger & William J. Broad, *Trump Inherits a Secret Cyberwar on North Korea*, N.Y. TIMES, Mar. 5, 2017, at A1.

[15] *See* Kim Zetter, *That Insane, $81M Bangladesh Bank Heist? Here's What We Know*, WIRED (May 17, 2016, 7:00 AM), https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

[16] *Id.*

[17] *See* Michael Corkery, *An $81 Million Sneak Attack on the World Banking System*, N.Y. TIMES, May 1, 2016, at A1.

government of Bangladesh. Many were surprised that a nation-state could be the victim of this kind of cybertheft.

A more recent, widespread attack on critical infrastructure occurred in May 2017. Using malicious software known as WannaCry, hackers engaged in a cyberattack that affected Internet-linked networks in dozens of countries.[18] Among its effects, the attack shut down access to patient files in Britain's National Health Service and many of its hospitals.[19] The attacks also affected the Russian Interior Ministry, the German rail system, European telecommunications companies, and a Chinese airline.[20] WannaCry is a type of ransomware—a malicious program that encrypts files, folders, and drives on a computer.[21] Once the ransomware is in place, the hackers demand payment of a ransom for a key to unlock the encryption.[22] Ransomware attacks are common, but the WannaCry attack attracted wide attention because the victims were located all over the world and were high profile, sophisticated institutions at the heart of critical infrastructure systems.[23]

Just a month later, in June 2017, another ransomware attack, which was described as an improved and more dangerous version of WannaCry, affected critical infrastructure systems around the world.[24] The attack caused the shutdown of bank ATMs in Ukraine, the disruption of payment mechanisms on the Kiev metro, and the shutdown of all computers at a Ukrainian electrical power company.[25] The attack then spread beyond Ukraine. The attack caused a Russian bank to close all its offices, forced hospitals in Pennsylvania to cancel operations, and demanded ransom from a chocolate factory in Australia.[26] As if further demonstration was necessary to prove the

---

[18] *See* Nicole Perlroth & David E. Sanger, *Hackers Use Tool Taken From N.S.A. in Global Attack*, N.Y. TIMES, May 13, 2017, at A1; *see generally Electronic Bandits*, ECONOMIST, May 2017, at 70.

[19] Russell Goldman, *Ransomware: How Hackers Hold Data Hostage*, N.Y. TIMES, May 13, 2017, at A9.

[20] *Id.*

[21] *See Electronic Bandits*, *supra* note 18.

[22] *Id.*

[23] *Id.*

[24] *See* Nicole Perlroth et al., *Cyberattack Hits Ukraine, Then Spreads*, N.Y. TIMES, June 28, 2017, at A1.

[25] *Id.*

[26] *Id.* The cyberattack also affected the operations of Maersk, one of the largest ocean freight transport companies. Maersk estimated that it lost as much as $300 million as a result of the loss of business caused by the attack. *See* Jordan Novet, *Shipping Company Maersk Says June Cyberattack Could Cost It up to $300 Million*, CNBC (Aug. 16, 2017,

prevalence and potential dangers posed by cyberattacks, July 2017 brought several media reports of attacks on electric utilities in the United States.[27] The most notable instance was an attempt to breach the network at a nuclear power plant in Kansas.[28] According to government agencies, public safety was never in danger. Nonetheless, these reports confirm the constant threat to critical infrastructure systems.

Nation-states themselves conduct cyberattacks. The United States has reportedly conducted cyberattacks on North Korea to damage its nuclear missile program.[29] In the past few years, a large number of North Korea's rockets have unexpectedly exploded, veered off course, or disintegrated in midair and plunged into the sea.[30] Some observers believe that such failures are the result of American cyberattacks, but this has not been confirmed, and some doubt America has the capability to cause such failures.[31] A more widely known cyberattack occurred with the use of the Stuxnet virus, which damaged Iran's nuclear program. In June 2009, someone introduced a destructive digital worm into the computer network controlling Iran's nuclear enrichment program.[32] Stuxnet was the "world's first real cyberweapon."[33] Unlike other worms or viruses, Stuxnet did not simply hijack targeted computers or steal information; it physically destroyed equipment controlled by the computers.[34] Stuxnet physically destroyed hundreds of centrifuges, which are necessary pieces of equipment to make nuclear weapons.[35] It is widely assumed

---

2:04 PM), https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.

[27] *See, e.g.*, Nicole Perlroth, *Hackers Are Targeting Nuclear Plants, U.S. Says*, N.Y. TIMES, July 7, 2017, at B5 (While the reports were published in July 2017, it is unclear when the attacks occurred.).

[28] *See id.*

[29] *See* Sanger & Broad, *supra* note 14.

[30] *Id.*

[31] *Id.*

[32] *See* Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011, 7:00 AM), https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

[33] *Id.*

[34] *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[35] *See id.* "Centrifuges are large cylindrical tubes—connected by pipes in a configuration known as a 'cascade'—that spin at supersonic speed to separate isotopes in uranium gas for use in nuclear power plants and weapons." *Id.* The centrifuges were governed by a control system supplied by Siemans, a large German industrial/technology

that Stuxnet was developed by the United States and Israel, although that has never been publicly confirmed.[36]

The shutdown of a power grid, the theft of millions of dollars from a central bank, and the attacks on nuclear weapons programs share a common thread—they all were cyberattacks on a country's critical infrastructure. The threats are real, not hypothetical, and exist today, not somewhere in the future. Cyberattackers possess the capability to cause oil spills (by attacking pipelines or refineries), power generator explosions, train derailments, airplane crashes, and missile detonations.[37] The vital roles that critical infrastructure systems play in the necessary functions of a society means that any disruption or damage could cripple it. The Critical Infrastructures Protection Act of 2001 defines critical infrastructure (CI) as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[38] The Department of Homeland Security (DHS) adopts this definition as well.[39] DHS identified sixteen critical infrastructure sectors. They are the (1) chemical sector; (2) commercial facilities sector; (3) communications sector; (4) critical manufacturing sector; (5) dams sector; (6) defense industrial base sector; (7) emergency services sector; (8) energy sector; (9) financial services sector; (10) food and agriculture sector; (11) government facilities sector; (12) healthcare and public health sector; (13) information technology sector; (14) nuclear reactors, materials and waste sector; (15) transportation systems sector; and (16) water and wastewater systems sector.[40] Cybersecurity threats to critical infrastructure have the potential to (1) cripple or destroy an individual business; (2) cripple or destroy the ability to provide basic public services on a local, regional, or national

---

firm (the controller is called the Process Control System 7). *See* William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1. Stuxnet targeted and took over control of the Siemans controllers, which in turn caused the centrifuges to spin at a rate that caused them to physically destruct. *Id.*

36 *See* Broad et al., *supra* note 35.

37 *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 70 (2010).

38 Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c(e) (2012).

39 U.S. Dep't of Homeland Sec., *What is Critical Infrastructure?*, HOMELAND SECURITY, https://www.dhs.gov/what-critical-infrastructure (last updated July 12, 2017).

40 U.S. Dep't of Homeland Sec., *Critical Infrastructure Sectors*, HOMELAND SECURITY, https://www.dhs.gov/critical-infrastructure-sectors (last updated July 11, 2017).

scale; and (3) cause loss of property or even loss of life, perhaps on a catastrophic scale. Cyberattacks on CI have occurred and continue to occur. CI is particularly at risk because most of it is owned by the private sector, with private owners utilizing different security practices.[41]

Electric power grids, communications networks, air traffic control systems, maritime navigation systems, and bank payment systems are just a few examples of CI owned by the private sector. Everyone depends on these systems for safety, health, and welfare. Typically, one would expect the government to be in charge of protecting systemically crucial systems. For example, people do not expect the private sector to provide an army or a navy. But most CI systems are provided by private entities that are responsible for protecting their own systems. While some cyberattacks are personally intrusive and violate privacy, this Article addresses the kinds of cyberattacks that can cause catastrophic loss of life and property, and it discusses the consequences of the fact that most CI systems are privately owned.

> Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)–most of which is held by the private sector–could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare successful attack with high impact can pose a larger risk than a common successful attack with low impact.[42]

The aviation industry provides an illustration of systemic vulnerabilities that have analogues in a wide range of CI systems. Aviation relies on interconnected networks of electronic systems. An airport relies on such networks to operate its security, power, fueling, and aircraft maintenance systems.[43] The air traffic control system relies on Internet Protocol (IP) networking to communicate.[44] The operation of an aircraft depends upon systems connected to multiple networks.[45] A passenger jet is vulnerable to interference with its flight

---

[41] Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 767 (2016).

[42] FISCHER, *supra* note 2, at 3.

[43] *See* Andrew V. Schmidt, Note, *Cyberterrorism: Combating the Aviation Industry's Vulnerability to Cyberattack*, 39 SUFFOLK TRANSNAT'L L. REV. 169, 187 (2016).

[44] *Id.* at 188–89.

[45] *See generally* INT'L GRP. OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 259 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0]. The predecessor of the *Tallinn Manual 2.0* was published in 2013. It was called the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, and was the "product of a three-year project by twenty

control systems and its onboard navigation and communications systems.[46] A Boeing 777 has over three million parts produced by 500 suppliers, and many of these parts are linked through electronic networks connected to the Internet.[47] Anything connected to the Internet is exposed to cyberattack.[48] Points of connection pose

---

renowned international law scholars and practitioners" and "identifies the international law applicable to cyber warfare and sets out ninety-five 'black-letter rules' governing such conflicts." INT'L GRP. OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, at opening page (Michael Schmitt ed. 2013) [hereinafter TALLINN MANUAL]. The *Tallinn Manual 2.0* supersedes the *Tallinn Manual*. *See* TALLINN MANUAL 2.0, *supra*, at 1–2.

46 TALLINN MANUAL 2.0, *supra* note 45, at 259.

47 Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 FIU L. REV. 635, 641 (2015) [hereinafter Shackelford & Russell, *Above the Cloud*].

48 *See* Peter Haynes & Thomas A. Campbell, *Hacking the Internet of Everything*, SCI. AM. (Aug. 1, 2013), https://www.scientificamerican.com/article/hacking-internet-of-everything/. Generally, devices are connected to the Internet through servers, including web servers.

> Internet servers make the Internet possible. All of the machines on the Internet are either servers or clients. The machines that provide services to other machines are servers. And the machines that are used to connect to those services are clients. There are Web servers, e-mail servers, FTP servers and so on serving the needs of Internet users all over the world.

Jeff Tyson, *How Internet Infrastructure Works*, HOWSTUFFWORKS, https://computer.howstuffworks.com/internet/basics/internet-infrastructure9.htm (last visited Nov. 11, 2017). The web server is comprised of the hardware, operating system, web server software, TCP/IP protocols and site content, which together enable delivery of information from the Internet to the browser. *Definition of: Web Server*, PCMAG., http://www.pcmag.com/encyclopedia/term/54342/web-server (last visited Nov. 5, 2017). Attacks on web servers are a common form of cyberattack. *Cyber Security*, BERKELEY LAB, https://commons.lbl.gov/display/cpp/Web+Server+Requirement%3A+OS+and+Application (last visited Nov. 5, 2017). The Federal Communications Commission issued a warning to small businesses about attacks on web servers: "Web servers, which host the data and other content available to your customers on the Internet, are often the most targeted and attacked components of a company's network." FCC, CYBER SECURITY PLANNING GUIDE WS-1 (2012), https://transition.fcc.gov/cyber/cyberplanner.pdf.

The following are examples of specific security threats to web servers:

- Cyber criminals may exploit software bugs in the web server, underlying operating system, or active content to gain unauthorized access to the web server. Examples of unauthorized access include gaining access to files or folders that were not meant to be publicly accessible and being able to execute commands and/or install malicious software on the web server.
- Denial-of-service attacks may be directed at the web server or its supporting network infrastructure to prevent or hinder your website users from making use of its services. This can include preventing the user from accessing email, websites, online accounts or other services. The most common attack occurs when the attacker floods a network with information, so that it can't process the user's request.

vulnerabilities and require cybersecurity defenses. The potential exists to endanger a single aircraft or even the air traffic control system through a cyberbreach.[49]

A basic challenge in cybersecurity is the fact that approximately eighty-five percent of America's CI is owned by the private sector.[50] The CI systems are owned and operated by thousands of businesses, which in turn may have thousands more private entities who either supply, service, or access the CI systems. The national cybersecurity framework relies on private actors to invest in a sufficient amount of cybersecurity measures to avoid catastrophic damage to CI. However, few private entities are required by law to implement any particular level of cybersecurity.[51] Thus, it is not surprising that many experts

---

- Sensitive information on the web server may be read or modified without authorization.
- Sensitive information on backend databases that are used to support interactive elements of a web application may be compromised through the injection of unauthorized software commands. Examples include Structured Query Language (SQL) injection, Lightweight Directory Access Protocol (LDAP) injection and cross-site scripting (XSS).
- Sensitive unencrypted information transmitted between the web server and the browser may be intercepted.
- Information on the web server may be changed for malicious purposes. Website defacement is a commonly reported example of this threat.
- Cyber criminals may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the web server.
- Cyber criminals may also attack external entities after compromising a web server. These attacks can be launched directly (e.g., from the compromised server against an external server) or indirectly (e.g., placing malicious content on the compromised web server that attempts to exploit vulnerabilities in the web browsers of users visiting the site).
- The server may be used as a distribution point for attack tools, pornography or illegally copied software.

Id.

[49] With such dangers in mind, the German military launched a new cybersecurity initiative in 2017 to protect its aviation system. Andrea Shalal, *German Military Aviation Command Launches Cyber Threat Initiative*, REUTERS (July 12, 2017, 11:12 AM), http://www.reuters.com/article/us-germany-military-cyber-aviation-idUSKBN19X2J6?utm_source=twitter&utm_medium=Social. The initiative was motivated, in part, by a demonstration of a hacker's ability to take control of an aircraft, and the industry's adoption of communication protocols similar to those used on the internet to connect cockpits, cabins and ground controls, which expose air traffic to vulnerabilities. *Id.*

[50] *See* Sales, *supra* note 12, at 1506.

[51] *Id.* One important exception applies to private firms that contract with the Department of Defense (DOD) in certain situations. For example, the DOD published an interim final rule, which requires contractors to comply with certain cybersecurity requirements specified by the National Institute for Standards and Technology. Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and

describe the state of cybersecurity defenses for CI as "inadequate."[52] The government does not impose security requirements, leaving it to the private-sector entities to set their own practices and policies for protecting their computer systems.[53]

At this point, a summary of statutory definitions and loose, working definitions is necessary. This Article uses the term "cyberspace" to mean "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[54] "Cybersecurity" is used generally to mean (1) "[a] set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software and the information they contain and communicate, including software and data, as well as other elements of cyberspace"; (2) "[t]he state or quality of being protected from threats"; and (3) "[t]he broad field of endeavor aimed at implementing and improving those activities and quality."[55] This Article also adopts the definition of "cyberattack" used by the United States military:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure . . . . A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human

---

Contracting for Cloud Services,.80 Fed. Reg. 51,739 (effective Aug. 26, 2015) (interim rule). The National Institute for Standards and Technology and its role in cybersecurity is discussed in Part II. This particular requirement has the goal of safeguarding access to the Cloud by contractors. *Id.*

52 *See* Sales, *supra* note 12, at 1506.

53 *Id.*

54 *See* THE WHITE HOUSE, NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD-54 3 (Jan. 8, 2008), https://fas.org/irp/offdocs/nspd/nspd-54.pdf (so defining).

55 FISCHER, *supra* note 2, at 1. There is no agreed upon meaning of the term; it serves more as a loose reference. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 291 (2014) ("there is surprising disagreement" as to precise definitions). A similar working definition of cybersecurity is "the policy field concerned with managing cyber threats, including unauthorized access, disruption, and modification of electronically stored information, software, hardware, services, and networks." Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 311–12 (2015) [hereinafter Shackelford et al., *Global Cybersecurity*].

> operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from delivery.[56]

The Cybersecurity Information Sharing Act of 2015 (CISA) also sets forth important definitions.[57] It defines "cybersecurity purpose" to mean "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[58] It also defines "cybersecurity threat" to mean

> an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.[59]

Part I of this Article explains that cybersecurity protection of CI is a "public good." This is important because a market economy faces inherent barriers to providing public goods. In general, public goods are things or situations that provide a widespread benefit available to all. The economic problem they pose, however, is that any person providing a public good is unable to capture the full economic benefit or profit of providing the good. This means there is little economic or profit incentive to do so, which results in the less than optimal supply of such goods. This conundrum describes the problem in protecting CI. Part II presents an overview of the state of America's cybersecurity laws and the government's efforts to promote strong cybersecurity for CI. The government's approach is to encourage voluntary responses by the private sector to improve cybersecurity (in contrast to imposing mandates). Part III explains why the government has chosen a voluntary approach in this area and discusses reasons why such an approach is rational and/or desirable. However, there are significant problems with this approach. Thus, Part IV discusses the disadvantages of relying on voluntary efforts by the private sector to provide a public good. A major problem is the significant market disincentive to any private entity that is in a position to supply a public good. The market is unable to provide a profit incentive to a

---

[56] Memorandum from James E. Cartwright, Gen., United States Marine Corps and Vice Chairman of the Joint Chiefs of Staff, on Joint Terminology for Cyberspace Operations to Chiefs of the Military Services (2010), http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[57] 6 U.S.C. § 1501 (2012) (effective Dec. 18, 2015).

[58] *Id.* § 1501(4).

[59] *Id.* § 1501(5)(A).

private supplier of a public good because the supplier generally cannot capture the profit/benefit of public goods they supply. This results in market failure—the inability of a free market to supply the optimal amount of a public good.[60] Market failures for public goods have traditionally been addressed by government-based solutions.[61] In line with this approach, Part V presents a modest proposal to improve cybersecurity based on expanding already established subsidies to encourage and facilitate additional spending on cybersecurity by private entities. A few summary observations are set forth in the Conclusion.

I
CYBERSECURITY AND PROTECTION OF CRITICAL INFRASTRUCTURE AS A PUBLIC GOOD

Protection of CI from cyberattacks is a matter of national security. The Department of Homeland Security makes that clear in its definition of CI. President Obama described cybersecurity as "one of the most serious economic and national security challenges we face as a nation."[62] This challenge is due to the increasingly important role of the Internet for personal, business, and government use. The Internet is inseparable from numerous CI systems and is in itself CI.[63]

---

[60] *See* Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 929–30 (2005) (discussing market failure for infrastructure).

[61] *Id.* at 925.

[62] President Barack Obama, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

[63] *See* Frischmann, *supra* note 60, at 920.

> The Internet meets all three demand-side criteria for infrastructure. The Internet infrastructure is a partially (non)rival good; it is consumed both nonrivalrously and rivalrously, depending upon available capacity. The benefits of the Internet are realized at the ends. Like a road system, a lake, and basic research, the Internet is socially valuable primarily because of the productive activity it facilitates downstream. That is, end-users hooked up to the Internet infrastructure generate value and realize benefits through the applications run on their computers and through the consumption of content delivered over the Internet . . . . The Internet currently is a mixed commercial, public, and social infrastructure.

Id. at 1006.

National security (which includes cybersecurity protection of CI) is a public good.[64] A public good is a thing or condition that benefits all members of a society.[65] Infrastructure, in all forms, generates public goods.[66] To use the scholarly jargon, a public good is something that is both nonexcludable and nonrivalrous.[67] A good is nonexcludable if

---

[64] *Public Goods - The Economic Lowdown Podcast Series, Episode 17*, FED. RES. BANK ST. LOUIS, https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-17-public-goods (last visited Nov. 11, 2017) [hereinafter *Public Goods Podcast*].

[65] *See* Lawrence Solum, *Legal Theory Lexicon: Public and Private Goods*, LEGAL THEORY BLOG, (June 19, 2016, 10:47 AM), http://lsolum.typepad.com/legaltheory/2016/06/legal-theory-lexicon-public-and-private-goods.html (explaining that "[t]he phrase 'public good' or 'public goods shall be used . . . to refer to the economists' idea of goods (in the broad sense that includes both 'goods' and 'services')").

[66] *See* Frischmann, *supra* note 60, at 931–32.

[67] *See Public Goods Podcast*, *supra* note 64; *see also* Solum, *supra* note 65. Solum provides:

> There are two criteria by which public goods are distinguished from private goods. A good is public only if it is both nonrivalrous and nonexcludable. A good is private only if it is both rivalrous and excludable. (We will deal with the mixed cases in just a bit.)
>
> "Rivalrousness" is a property of the consumption of a good. Consumption of a good is rivalrous if consumption by one individual X diminished the opportunity of other individuals, Y, Z, etc., to consume the good. Some goods are rivalrous because they are "used up." If I drink a glass of Heitz Martha's Vineyard, then you cannot drink that same glass of wine. If I set off a firecracker, you cannot set off the same firecracker. Other goods are rivalrous because of crowding effects. If I am using the free internet terminal at the student lounge, then you cannot use the same time slice of the terminal—because only one person can sit in front of the screen at the same time.
>
> "Excludability" is also a property of consumption of a good. It is helpful to distinguish two forms of excludability: (1) excludability through self help, and (2) excludability through law. If I want to exclude you from my land, I can build a fence—the exclusion results from self help. But if I want to exclude you from copying a novel that I've written and I want to make the novel generally available for sale, self help will not work. (It would be ridiculously expensive to hire a guard to monitor each copy or every photocopy machine.) Government, however, can make unauthorized copying a criminal offense or actionable civil wrong, thereby creating exclusion through law.

Solum, *supra* note 65.

> Nonrivalry is a key economic concept that one must appreciate when analyzing social welfare from a utilitarian perspective. Synonymous with indivisibility of benefits, nonrivalry describes the situation "when a unit of [a] good can be consumed by one individual without detracting, in the slightest, from the consumption opportunities still available to others from that same unit." For economists, "consumption" simply refers to the realization of benefits by virtue of one's access to the good.

Frischmann, *supra* note 60, at 942 (quoting RICHARD CORNES & TODD SANDLER, THE THEORY OF EXTERNALITIES, PUBLIC GOODS, AND CLUB GOODS 8 (1996)).

one is unable to prevent others from consuming or using it.[68] A good is nonrivalrous if one person's consumption does not negatively affect anyone else's consumption of the good.[69] The benefit accrues to each individual whether he pays for it or not and is not diminished by anyone else's enjoyment or consumption. The phrase "public good" is not limited to things that physically exist; it includes services and intangible benefits. To illustrate, the eradication of a disease is a nonexcludable good because one is unable to prevent others from benefiting from it. Nice weather is a nonrivalrous good because one person's enjoyment of the weather does not mean there is less nice weather for others. By contrast, a pie is not a public good. One is able to prevent others from eating the pie, so it does not possess the characteristic of nonexcludability. The pie also does not qualify as a nonrivalrous good because if one person eats the pie, no one else can.

An often-used example of a public good is national security.[70] National security is nonexcludable because if another country tried to invade California, the military would act to protect it regardless of whether individual Californian citizens paid their taxes.[71] It is nonrivalrous because one person's use of the public good does not

---

[68] *See* Solum, *supra* note 65.

[69] *Id.*

[70] Professor Solum explains,

> • Public goods have two characteristics—nonrivalrousness and nonexcludability. For example, consumption of national defense is nonrivalrous (my being protected by the U.S. armed forces doesn't diminish your protection). National defense is a nonexcludable good: the Army cannot say to Mexico, "Solum hasn't paid his national defense bill, Go ahead and attack him."
>
> • Private goods are rivalrous and excludable. If I own a laptop computer, my use of it diminishes your ability to use it; therefore, my consumption of the laptop rivals yours. Moreover, I can exclude you from the use of my laptop (by locking it up when I am not using it).

Id.

> National security is an example of a public good. We all benefit from this government service with hardly a second thought. We pay our taxes to the government, and the government uses part of those funds to defend the country from foreign and domestic threats. National security is nonexcludable because there is no way of withholding protection from those who don't pay taxes. If a missile were heading for the country, the military would shoot it down to save everyone in its path, regardless of who did and didn't pay their taxes. National defense is nonrival because one person's use of it does not hinder anyone else's consumption. For example, as the population grows, more people benefit from national security, but the level of protection for those already benefiting remains the same.

Public Goods Podcast, *supra* note 64.

[71] *See Public Goods Podcast*, *supra* note 64.

hinder anyone else's consumption; one person's enjoyment of national security does not mean there is less protection for others.[72]

National security is provided by the federal government at taxpayer expense. Governments usually supply public goods.[73] A general principle of economics (and related legal theory) is that markets should provide private goods and government should provide public goods.[74] The reason for this is explained by economic theory.

Economic theory states that no rational person will voluntarily pay for a public good as long as someone else does. An individual enjoys clean air as long as someone else pays for the cost of clean air. An American within the United States is protected by America's antimissile defenses whether she pays taxes or not. This is the classic "free rider" problem.[75] Another aspect of this problem is that the free rider enjoys as much of the public good as someone who pays for it. Because no rational individual will voluntarily pay for a public good, societies turn to government to pay for public goods through taxes.

---

[72] *Id.*

[73] *Id.*

[74] *See* Solum, *supra* note 65.

[75] *Public Goods Podcast*, *supra* note 64.

> Free riders are the consumers who don't pay in order to consume the public good. Since public goods are free, most consumers become free riders because they have no incentive to pay the supplier. After all, consumers have a budget, so they won't likely pay for a good if they can get it for free. While there may be people who recognize the importance of a public good and have enough money to donate voluntarily, they form the exception to the rule. In general, people will not pay willingly for a public good.
>
> If a private business supplied a public good, most people would consume the product for free. Since it is nonexcludable and nonrival, consumers can already get the full benefits without paying anything. They won't likely donate much, if any, of their hard-earned cash. Hence, the company won't make much money. That's why private firms won't produce public goods; there's no reward. Firms instead spend their time and resources producing private goods because people do have to pay for those, allowing the firm to sell them for a profit.

Id.

> Some products, like national defense or police services, will not be produced in private markets because of what is called the "free-rider" problem. These products, called "public goods," have the unique character that consumption of them by one consumer does not diminish the possibility of consumption by another consumer. As a result, public goods must be purchased by the government if they are to be purchased at all. Otherwise, every consumer will attempt to become a free rider by waiting for someone else to purchase the product so that it can be used for free. Government regulation concerning the method and collection of taxes ensures that each citizen pays a share of the cost of governmental purchases of public goods.

RICHARD J. PIERCE, JR. ET AL., ADMINISTRATIVE LAW AND PROCESS 15 (6th ed. 2014).

In addition to the free rider problem, economic externalities also present an obstacle to the private sector providing goods. An economic externality is a cost generated by an activity that is not borne by the person or firm who engages in the activity.[76] An economic externality may also be described as "an effect on the market the source of which is external to the market."[77] It is "the imposition of a cost or benefit on a nonconsenting third party" by the party engaging in the economic activity.[78]

> Externalities can be either positive or negative. "Positive externalities occur whenever an activity generates benefits that the actor is unable to internalize," such as through prices; "[n]egative externalities occur when one's activity imposes costs on others" that likewise are not transmitted through prices. Economic theory predicts that the market will oversupply negative externalities relative to socially optimal levels "because the producer will internalize all benefits of the activity but not all the costs." It also predicts that the market will undersupply positive externalities because third parties will free ride. Externalities thus represent a form of market failure. The standard government response to a negative externality is to discourage the responsible conduct (e.g., with taxation or regulation); the standard response to a positive externality is to encourage the responsible conduct (e.g., with a subsidy).[79]

To illustrate, smoke from a factory chimney that blankets the surrounding area is a negative externality because it is a harm suffered by nonconsenting third parties caused by the economic activity of the factory.[80] Absent government intervention, the factory owner does not bear the cost imposed on others. In contrast, a world-famous museum that attracts visitors from around the world generates positive externalities. However, the museum is unable to capture the benefit that surrounding businesses enjoy for free (such as increased

---

[76] *See* Solum, *supra* note 65.

[77] *See* Sales, *supra* note 12, at 1519 (quoting Niva Elkin-Koren & Eli M. Salzberger, *Law and Economics in Cyberspace*, 19 INT'L REV. L. & ECON. 553, 563 (1999)).

[78] *Id.* at 1520.

[79] *Id.*

[80] An administrative law treatise states:

> If a manufacturing process, for example, produces toxic vapors that make persons ill, the manufacturer should pay for the medical expenses of those persons and include them as part of the price for which the product is sold. If the manufacturer does not pay those costs, the product will be overproduced. There will be more demand for the product than if it were sold at a higher price that reflected the damages its production caused.

PIERCE, JR. ET AL., *supra* note 75, at 15.

tourism and higher real estate prices) due to their proximity to the museum (absent government intervention).[81]

The protection of CI from cyberattacks presents a set of difficult problems. Protection of CI is a matter of national security and defense. It is a public good that benefits all. However, the government relies on private owners of CI to provide the public good even though there is little economic incentive to do so. Of course, self-protection provides an incentive to invest in cybersecurity, but the problem of externalities prevents the optimal amount of investment. In sum, the government looks to private businesses to provide a significant amount of national security. Approximately eighty-five percent of America's CI is owned by the private sector.[82] Despite the necessity of protecting CI, the government generally does not impose mandatory cybersecurity requirements or provide financial support for cybersecurity investment.[83]

> Cyber-security can be understood in these terms. If a company suffers an intrusion, much of the harm will fall on third parties; the attack results in a negative externality. It can be extraordinarily difficult to internalize these costs. The class of persons affected by the intrusion will often be so large that it would be prohibitively expensive to use market exchanges to internalize the resulting externalities; the transaction costs are simply too great. Nor can tort law internalize the costs, as firms generally do not face liability for harms that result from cyber-attacks on their systems or products. Because many companies do not bear these costs, they ignore them when deciding how much to spend on cyber-defense and therefore tend to underinvest relative to socially optimal levels. (This is true both of companies that produce computer products, such as software manufacturers, and companies that use them, such as ISPs and utility companies.) Cyber-security also involves positive externalities. A company that secures itself against intruders makes it harder for assailants to commandeer its systems to attack others. Investments in cyber-defense thus effectively subsidize other firms. Because the investing company doesn't capture the full benefit of

---

[81] In short, many other parties (including unidentifiable parties), other than the owner, benefit from infrastructure (critical or not).

> Whether we are talking about [museums], transportation systems, the electricity grid, ideas, environmental ecosystems, or Internet infrastructure, the bulk of the social benefits generated by these resources derives from their downstream uses. They create value downstream by serving a wide variety of end-users who rely on access to them. Yet social demand for the infrastructure itself is extremely difficult to measure.

See Frischmann, *supra* note 60, at 958.

[82] Sales, *supra* note 12, at 1506.

[83] *Id.*

> its expenditures, it has weaker incentives to secure its systems. And because other companies are able to free ride on the investing firm's expenditures, they have weaker incentives to adopt defenses of their own.[84]

To the extent private entities underinvest in cybersecurity for CI, negative externalities increase because the cost of a successful cyberattack will be borne by numerous unrelated third parties. Because the entity with weak cybersecurity will not bear all those costs, the amount of investment in cybersecurity will not incorporate the full, actual cost of potential harm. On the other hand, an optimal amount of investment in cybersecurity will lead to increased positive externalities because unrelated third parties will enjoy the benefits of safe CI systems. However, any entity that invests an adequate amount in cybersecurity will not be able to charge for the positive externalities it generates.

II
A BRIEF REVIEW OF AMERICA'S CYBERSECURITY LAWS

So what is the state of America's law regarding the protection of CI? One commentator described America's system of cybersecurity laws as a patchwork of related laws, much of which is focused on data breaches and privacy.[85] The United States does not have a unified, comprehensive approach to cybersecurity law and policy; the area is addressed through the jurisdiction of a variety of federal agencies, including the Department of Homeland Security, the Department of Defense, the National Security Agency, and the Federal Trade Commission.[86]

---

[84] *Id.* at 1520.

[85] Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 402 (2016).

[86] Scott J. Shackelford et al., *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 221 (2016) [hereinafter Shackelford et al., *"Voluntary" Cybersecurity Frameworks*]. One commentator observed (in response to a question about the state of U.S. cybersecurity law),

> After pausing for far too long, I said, "We don't really have any cybersecurity laws." What we have, instead, is a patchwork of related laws, including breach notification and privacy statutes, that focus on penalizing companies for inadequate data security. But our legal system lacks a coordinated network of laws that are designed to promote cybersecurity and prevent data breaches from occurring in the first place.

Kosseff, *supra* note 85, at 402. Kosseff added:

> As discussed above, the United States does not have a cohesive cybersecurity legal framework. Instead, it has a patchwork of laws that address some aspects of

A starting point for a brief review of U.S. cybersecurity law is the 2014 National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST Framework).[87] The goal of the

---

> data security. These laws fail to work together harmoniously, occasionally conflict, and do little to ensure the future security of data, networks, and systems. The current legal system largely is backward-looking, and provides companies and the public sector little guidance as to how to prevent future cybersecurity incidents.

Id. at 406. Johnson shares this assessment: "Cyberspace is governed by a patchwork of state, federal, and international regulations. Our fragmented regulatory framework, characterized by industry-specific legislation, leaves significant gaps in the oversight of cyberspace." Johnson, *supra* note 1, at 576. Other commentators note,

> In the private sector, federal statutes relating to cybersecurity are typically industry-specific and create general standards. In addition, the majority of these cybersecurity statutes are directed at health care entities and financial institutions. Again, while statutes were recently passed to facilitate private-public cooperation in establishing cybersecurity standards across critical infrastructure industries, they do not establish a comprehensive regulatory framework.

Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors*, 37 CARDOZO L. REV. 1827, 1839 (2016).

[87] NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [hereinafter NIST FRAMEWORK]. The NIST Framework was developed pursuant to President Obama's Executive Order 13636. *Id.* at 3. The Executive Summary opens by noting, "The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk." *Id.* at 1. The origins of cybersecurity law may be traced back to the 1986 U.S. Computer Fraud and Abuse Act, which criminalized unauthorized access and damage to computers and networks. *See* Amanda N. Craig et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 732 (2015). Subsequent federal legislation addressing cybersecurity include "the E-Government Act of 2002, the Cybersecurity Research and Development Act of 2002, the Federal Information Security Management Act of 2002, the Cyber Security Enhancement Act of 2002, the Cybersecurity Enhancement Act of 2014, and the National Cybersecurity Protection Act of 2014." Johnson, *supra* note 1, at 577. However, "no single piece of federal legislation exists that addresses cybersecurity threats and issues." *Id.* Another important piece of legislation was the Critical Infrastructures Protection Act of 2001. 42 U.S.C. § 5195c (2012). It states that it is the policy of the United States is to ensure

> (1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States;
> (2) that actions necessary to achieve the policy stated in paragraph (1) be carried out in a public-private partnership involving corporate and non-governmental organizations; and
> (3) to have in place a comprehensive and effective program to ensure the continuity of essential Federal Government functions under all circumstances.

NIST Framework is to guide "the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks."[88] Focus should be placed on "voluntary."[89] One goal of the NIST Framework is to promote the development of a standard of cybersecurity care in the United States by incorporating private industry best practices.[90] It seeks to encourage "a flexible and cost-effective approach to enhancing cybersecurity by assisting owners and operators of critical infrastructure in assessing and managing cyber risk."[91] Freedom and flexibility are the bases of the NIST Framework. It does not establish or prescribe the amount of cyber-risk the private sector should tolerate in a given segment of their operations. Instead of developing an entirely new set of standards, it "'relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience,' which allows the Framework to 'scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements.'"[92] The NIST Framework pursues the much more modest goal of providing a "common language" for entities to evaluate their current cybersecurity needs and vulnerabilities, determining the likelihood of attacks, and prioritizing opportunities for internal and external stakeholders about cybersecurity risk.[93]

At first glance, it may seem strange that such a vital aspect of national security should be left to voluntary efforts by the private sector. An alternative approach would have the federal government set mandatory standards and requirements for the establishment and implementation of cybersecurity protection of CI. However, there are strong policy reasons that support a voluntary approach, and strong arguments against mandatory federal requirements. First, the foremost experts and leaders of innovation usually work in the private sector, and technological advances often originate in the private sector. The

---

Id. § 5195c(c).

88 NIST FRAMEWORK, *supra* note 87, at 1.

89 *See* Shackelford et al., *"Voluntary" Cybersecurity Frameworks*, *supra* note 86, at 218 (describing America's protection of CI as "a largely voluntary approach through the National Institute of Standards and Technology supplemented by sector-specific regulation and U.S. Cyber Command").

90 *See id.* at 221.

91 *Id.* at 222.

92 *Id.* at 223.

93 *Id.*

leaders of the private sector, as a group, have superior expertise and knowledge to that of government officials.

Second, technology develops and improves at a rapid pace, so it is likely that any set of mandatory regulations would be obsolete by the time they become effective. The private owners of CI could find themselves being forced to comply with outdated technology standards when state of the art technology is available.[94] Basing CI protection on a voluntary approach preserves the private sector's freedom to improve as rapidly as the technology advances and avoids problems created by inflexible or outdated regulatory requirements.[95]

With such policy considerations in mind, the NIST Framework avoided imposing mandates on the private sector. Its Executive Summary states,

---

[94] A student note described the problem in this way:

> However, the private sector is generally wary of additional cybersecurity laws or regulations that might mandate specific standards or technology. The private sector puts forth four main arguments against regulations and broadly-scoped legislation. First, such requirements could increase business expenses and overhead as well as misallocate company resources. Second, companies would be forced to focus on compliance with measures that quickly become out-of-date and ineffective, rather than on methods to address current and future threats. Third, such requirements would disincentivize the public-private partnerships that are already addressing the challenges. Fourth, the regulations would not necessarily improve cybersecurity, particularly when the government does not have a great track record for protecting against cyber breaches.

Chris Laughlin, Note, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations are Effective*, 14 COLO. TECH. L.J. 345, 357 (2016). Other commentators have noted that imposing mandatory requirements on private entities regarding cybersecurity defenses would be counterproductive because of the possibility that the government standards would be below the level of security already implemented by private business. *See* Garrie & Reeves, *supra* note 86, at 1839 n.62.

[95] *See* Shackelford et al., *Global Cybersecurity*, *supra* note 55, at 309. The ability to respond rapidly to cyberthreats is crucial. CI owners suffer repeated cyberattacks, and some electric utilities report being probed thousands of times each month. *See* Shackelford et al., *Sustainable Cybersecurity*, *supra* note 14, at 2005–06.

> Cybersecurity is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with an access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition processes and previously unknown, or zero-day, vulnerabilities with no established fix. Even for vulnerabilities where remedies are known, they may not be implemented in many cases because of budgetary or operational constraints.

FISCHER, *supra* note 2, at 2.

> The Framework enables organizations–regardless of size, degree of cybersecurity risk, or cybersecurity sophistication–to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure . . . .
>
> The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks–different threats, different vulnerabilities, different risk tolerances–and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.[96]

By design, the NIST Framework provides a voluntary procedure for private-sector entities to determine and implement cybersecurity best practices without imposing regulatory requirements.[97]

This voluntary approach to protection of CI is embodied in recent federal legislation addressing cybersecurity. The Cybersecurity Act of 2015 became law on December 18, 2015.[98] It establishes a voluntary information-sharing framework designed to encourage the private and public sectors to share cyberthreat information.[99] The Act instructs the federal government "to establish procedures for sharing classified and unclassified cyberthreat indicators and defensive measures with the private sector."[100] The Department of Homeland Security is responsible for creating a mechanism for the government to receive notifications of cyberthreat indicators and defensive measures from the private sector and then sharing that information with other government entities.[101] The emphasis on public-private sector cooperation makes sense and is necessary given the public-private nature of the Internet itself. The open architecture of the Internet makes it pointless to try to isolate or draw clear lines between private sector concerns and public sector concerns.[102]

Title I of the Cybersecurity Act of 2015 contains the Cybersecurity Information Sharing Act of 2015 (CISA).[103] The purpose of CISA is

---

96 NIST FRAMEWORK, *supra* note 87, at 1–2.

97 *See* Shackelford et al., *Global Cybersecurity*, *supra* note 55, at 308–09.

98 Cybersecurity Act of 2015, Pub. L. No. 114–113, 129 Stat. 2242 (2015).

99 *See* Kelly Russo & Harvey Rishikof, *Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics*, 19 CHAP. L. REV. 421, 433 (2016).

100 *Id.*

101 *Id.*

102 Kosseff, *supra* note 85, at 404.

103 6 U.S.C. § 1501 (2012) ("This title [enacting this subchapter . . .] may be cited as the Cybersecurity Information Sharing Act of 2015."). The Cybersecurity Act of 2015

to improve cybersecurity defenses in the United States by creating "a voluntary cybersecurity information sharing exchange designed to encourage public and private-sector actors to share cyber threat information."[104] CISA is designed to facilitate and promote "the timely sharing of . . . cyber threat indicators and defensive measures in the possession of the Federal Government with . . . non-Federal entities."[105] CISA makes clear, however, that private-sector involvement is voluntary.[106] It provides, "Nothing in this subchapter shall be construed to permit a Federal entity . . . to require a non-Federal entity to provide information to a Federal entity or another non-Federal entity . . . ."[107] It further provides, "Nothing in this subchapter shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this subchapter."[108] The text expressly and repeatedly emphasizes the voluntary nature of the legislation.

---

contains four titles. Title I addresses the private sector and establishes a centralized mechanism for information sharing. Title II instructs DHS to improve cybersecurity within the federal government and to implement Title I. Title III calls for a cybersecurity assessment of the federal workforce. Title IV provides for other measures related to threats to critical information systems and networks. Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242.

[104] *See* Johnson, *supra* note 1, at 578.

> "Information sharing is one of the most potent tools we have to counter malicious cyber activity," Julia Philipp, deputy director for cyber intelligence and head of the financial sector Cyber Intelligence Group at the U.S. Department of the Treasury, said at a recent conference. "Malicious cyber actors share information and tools used to exploit our systems every day; we should be doing the same to stop them."

See Sean McMahon, *Four Keys to Winning the Cyber Arms Race*, BLOOMBERG (Apr. 20, 2015), https://www.bloomberg.com/vault/blog/four-keys-to-winning-the-cyber-arms-race/.

[105] 6 U.S.C. § 1502(a)(1) (2012). A "non-Federal entity" includes "any private entity." *Id.* § 1501(14)(A). A private entity "means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof." *Id.* § 1501(15)(A).

[106] "It is important to note that CISA is strictly voluntary, i.e., there is no duty to share. It expressly prohibits the federal government from coercing parties into sharing. It also provides a safe harbor for participating entities, when they share information according to CISA's provisions. . . ." Jasper L. Tran, *Navigating the Cybersecurity Act of 2015*, 19 CHAP. L. REV. 483, 486 (2016).

[107] 6 U.S.C. § 1507(h)(1).

[108] *Id.* § 1507(i).

III
THE ADVANTAGES TO A VOLUNTARY APPROACH TO PROTECTION OF CI

There are millions of connections to the Internet, through a wide range of devices. The parties connected to the Internet include private individuals, small businesses, large businesses, and governments. The parties that make Internet-connected products are similarly diverse. Given this wide range, it seems prudent to avoid seeking a strict regulatory regime to govern all users, providers, and beneficiaries of CI connected to the Internet. There are clearly dangers of regulatory overreach when trying to fashion a coherent set of rules to apply to such a wide range, and conventional regulatory schemes may be ineffective. The nature of the Internet and cyberspace poses unique challenges.

> Cyberspace, by its very architecture, is a network of both private-sector and public-sector infrastructure. Unlike traditional regulatory area, such as food safety, where the government is more than an overseer of the private sector, the government is a partner with the private sector. The government developed the initial infrastructure of the Internet, and the private sector invested billions of dollars to build that initial infrastructure into the transformative force that it is today. Accordingly, unlike other areas, in which traditional top-down regulation is effective, cybersecurity requires a different mindset. Cybersecurity requires a continuation of the partnership between the government and companies. Indeed, an insecure Internet harms the private sector by slowing the growth and progress of the Internet; it is in the best interests of every company to work with the government for a more secure cyberspace.[109]

Thus, the nature of the public-private relationship is actually like a partnership:[110] partners need to work together, and one partner does not have the authority to command another partner.

One commentator has advanced several arguments against a mandatory regulatory regime, such as (1) cyberattacks do not pose an existential threat, (2) there are means other than regulation (such as subsidies and liability risks) to address cybersecurity, (3) regulations cannot keep up with the pace of technological advances, (4) no federal agency is suitable for leading a regulatory response, (5)

---

[109] Kosseff, *supra* note 85, at 411–12.

[110] The Critical Infrastructures Protection Act of 2001 actually uses the word "partnership" to describe the public-private relationship regarding cybersecurity. 42 U.S.C. § 5195c(c)(2) (2012).

lawmakers do not understand the nature of cybersecurity threats, (6) there are regulations already in place, and (7) American regulation will disrupt the global nature of the Internet.[111] These points raise a variety of issues, many of which are beyond the scope of this Article. However, they present colorable arguments in favor of a "voluntary" approach.

One point, in particular, is the inability to compare the cost versus benefit of increased cybersecurity. If the government is unable to calculate the benefit, it makes it difficult to justify requiring private entities to invest in a mandatory level of cybersecurity. Even a strong proponent of regulation, Professor Jack Goldsmith at Harvard, concedes that it is not possible to measure the cost of cybersecurity regulation versus the benefits.[112] Another scholar agrees that the benefits of cybersecurity and risks of cyberattacks are "impossible to

---

[111] *See* Paul Rosenzweig, *The Unpersuasiveness of the Case for Cybersecurity Regulation–An Introduction*, LAWFARE BLOG (May 17, 2012, 12:35 PM), https://www.lawfareblog.com/unpersuasiveness-case-cybersecurity-regulation-%E2%80%93-introduction. In his opposition to regulation, Mr. Rosenzweig argues: (1) More regulation is not necessary because cyber vulnerabilities of CI are not an existential threat; (2) Regulation is not the only way that governments deal with externalities. They can also be addressed through other means like subsidies, taxes, and the imposition of liability; (3) Regulation is an especially poor choice for use in a dynamic and changing environment where existing performance standards will almost certainly be irrelevant within a few years; (4) No Federal agency is suitable or designed to lead a comprehensive regulatory effort; (5) Regulations already exist in this sphere and have not been particularly effective; and (6) Additional federal regulation may have significant adverse effects on Internet governance, along with adverse cross-border effects. *Id.* These views are one side of the coin, and there are equally compelling counterarguments. For example, it seems surprising that anyone would doubt the existential threat posed by attacks on cyber vulnerabilities. President Obama did not seem to have such doubts.

> Much of our critical infrastructure—our financial systems, our power grid, health systems—run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before. Foreign governments and criminals are probing these systems every single day. We only have to think of real-life examples—an air traffic control system going down and disrupting flights, or blackouts that plunge cities into darkness—to imagine what a set of systematic cyber attacks might do. So this is also a matter of public safety.

Obama, *supra* note 62.

[112] Jack Goldsmith, *Response to Paul on Cyber-Regulation for Critical Infrastructure*, LAWFARE BLOG (May 21, 2012, 12:11 PM), https://www.lawfareblog.com/response-paul-cyber-regulation-critical-infrastructure ("in truth I do not know how to assess the costs of regulation versus the costs of non-regulation, and I have not seen any good analysis of that crucial issue in this context. Nor do I think such an analysis will be forthcoming, because so much information is classified, and because metrics are very hard in this context.").

measure precisely."[113] If this is indeed the case, then cybersecurity presents a highly challenging area to regulate because of the unknowability of benefits versus costs.[114] Because of the uncertainty over the benefits, efficacy, and effect on technological progress, perhaps the prudent course is to start with a voluntary, bottom-up approach.[115] There seem to be too many open questions regarding cost, benefit, and implementation for effective regulation. For example, the cost of a strong regulatory regime can partly be measured in dollar cost of things like upgrades, and compliance and legal fees. However, what is the corresponding dollar benefit? If the cost and benefit cannot be compared, how would a government justify a strong regulatory response?[116] The problem is aggravated if the cost

---

[113] Lawrence A. Gordon, Univ. of Md., Speaker at the International NCSC ONE Conference 2015: Investing in Cybersecurity: Insights from the Gordon-Loeb Model 4 (Apr. 13, 2015), https://www.rhsmith.umd.edu/files/Documents/SignatureEvents_Conferences_Symposiums_EventsNotSpecificToACenter/IBMWorkshop/2015/gordon.pdf.

[114] A cost-benefit analysis is a fundamental principle of administrative rulemaking.

> Cost-benefit analysis has . . . been elevated to the top of the administrative agenda by presidential orders that have tried to make comparison of costs and benefits a central element of federal regulation. On February 17, 1981, President Reagan issued Executive Order 12,291. It provides detailed procedures for issuance of so-called major regulations by executive branch regulatory agencies. All such agencies are required to prepare regulatory-impact analyses when they promulgate major rules. They must analyze the costs and benefits of the proposed regulations, and they are required to "maximize the net benefits to society." If the least-cost alternative has not been selected, the agencies are required to explain why.

BERNARD SCHWARTZ, ADMINISTRATIVE LAW 178 (3d ed. 1991). Thus, agencies are required to prepare a report on the costs and benefits of proposed regulations pursuant to presidential Executive Orders, and this is a generally accepted part of the administrative process. *See* PIERCE, JR. ET AL., *supra* note 75, at 86, 87, 434. However, only a few statutes expressly require an agency to prove that the benefits of a regulation exceed the costs. *Id.* at 437. Moreover, Congress has frequently rejected the use of cost-benefit analysis in many areas of heavily-regulated law. *Id.* at 435.

[115] The problem with a top-down approach was described this way:

> Too often government regulates through rigid commands, precluding industries from using more flexible and cost-effective measures that achieve the same goals. For example, in air and water pollution control, the rigid "best available technology" approach, which mandates control technologies for hundreds or even thousands of firms, gives industries little incentive to improve existing pollution control technologies. Incentive-based systems could save billions of dollars. Yet in spite of the potential advantages, efforts to seek better regulatory tools are hobbled by the statutory status quo, which either forbids such tools or engrafts them onto a bureaucratically complex system.

Cass R. Sunstein, *Congress, Constitutional Moments, and the Cost-Benefit State*, 48 STAN. L. REV. 247, 260 (1996).

[116] There is, of course, the case against over-reliance on cost-benefit analysis.

of strong regulation acts as an impediment to technological advances. In that situation, the costs could dangerously outweigh the benefits.[117] There is also uncertainty regarding both the extent and likelihood of harm. A cost-benefit analysis would need to factor in whether CI vulnerabilities pose an existential threat to systems, social order, and lives. If so, what is the likelihood of such a successful attack? Or is any attack on CI manageable, even if the likelihood of success is higher? These are necessary issues that need to be addressed when considering the type, extent, and strength of regulatory requirements. At a minimum, a basic expected value analysis would be one of the first steps. This type of analysis determines the likelihood of a particular threat and then multiplies that by the amount of estimated harm. However, if it is impracticable to supply reliable numbers into this calculation, then any result is unhelpful. It would be imprudent to impose regulatory mandates based on indeterminable data. Governments around the world confront the same issues regarding cybersecurity, and many have arrived at the same conclusion as the United States in not adopting top-down, command regulatory regimes.[118]

> Supporters of regulation counter that benefits do exceed costs for health and safety and environmental regulation, that a cost-benefit standard is an inappropriate measure of whether there should be regulation because it is extremely uncertain and biased, and that many forms of regulation have equitable goals which cannot be measured in economic terms.

PIERCE, JR. ET AL., *supra* note 75, at 16.

[117] The danger of unintended effects is an inherent risk in any regulatory scheme.

> Many regulatory initiatives result in harmful unintended consequences. Under the existing regulatory system, there is no systematic way to ensure that those consequences receive attention. Hence regulation tends to be based on partial perspectives that emerge from close attention to mere pieces of complex problems. This myopic approach ignores the importance of ensuring that regulation does not have unexplored side-effects or increase harms or risks on balance.

Sunstein, *supra* note 115, at 261–62. This passage neatly describes the problem regarding cybersecurity regulation. The need for a stronger legal framework may be driven by anecdotal accounts of well-publicized data breaches, as opposed to a systemic study of the problem. Indeed, it is frustrating that experts cannot even agree if cyberattacks pose existential threats.

[118] *See* Shackelford et al., *"Voluntary" Cybersecurity Frameworks*, *supra* note 86, at 218–19.

> The Cybersecurity Framework takes a risk-based approach for organizations to detect, mitigate, and respond to cyber threats. Rather than developing new cybersecurity standards and risk management processes, the Cybersecurity Framework "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience," which allows the

Another advantage of a voluntary approach is that it provides flexibility and the ability to adapt rapidly to new threats. Cyberattacks and cybersecurity are not static concepts. The creation of new forms of threats are limited only by the imagination of the hackers. As soon as cybersecurity experts can thwart a particular type of threat, new threats will spring up to evade the newly developed defenses. This cycle of attack and response is like an infinite loop. It would be extremely difficult for a "hard" regulatory approach based on top-down mandates by the federal government to adapt at the speed necessary to match the ongoing battle between hackers and cybersecurity defenses.

Other incentives encourage the development of strong cybersecurity defenses. Lawsuits from highly publicized breaches provide one form of incentive. For example, Target paid $39 million to settle a class action lawsuit resulting from the cybersecurity breach of its customers' personal information.[119] Sony paid nearly $8 million to settle a lawsuit filed by employees whose personal information was stolen through a cyberattack.[120] Thus, America's tort system provides

---

> Framework to "scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements." The Cybersecurity Framework provides a "common language" for entities to evaluate their current cybersecurity posture, determine their targeted state for cybersecurity, prioritize opportunities for improvement, assess progress toward their targeted state, and establish sufficient methods of communication among internal and external stakeholders about cybersecurity risk.

Shackelford et al., *Global Cybersecurity*, *supra* note 55, at 329–30 (quoting NIST FRAMEWORK, *supra* note 87, at 1).

> The Cybersecurity Enhancement Act of 2014 obligated NIST to coordinate with industry leaders and critical infrastructure owners to facilitate and support the development of an industry-led set of standards and procedures to reduce cyber risks to critical infrastructure. Part of the Act requires NIST to consult with government agencies in an attempt to coordinate the cybersecurity efforts between public and private sectors. The Act further requires NIST to work with industry leaders to "identify a prioritized, flexible, repeatable, performance-based, and cost-effective" set of standards that "owners and operators of critical infrastructure" can adopt to help "identify, assess, and manage cyber risks."

Garrie & Reeves, *supra* note 86, at 1845 (quoting Cybersecurity Enhancement Act, 15 U.S.C. § 272(e)(1)(A)(ii) (2012)).

[119] Ahiza Garcia, *Target Settles for $39 Million over Data Breach*, CNNMONEY (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/.

[120] Nate Raymond, *Sony Settles Employees' Suit Over 'The Interview' Data Breach for $8 Million*, INS. J. (Oct. 21, 2015), http://www.insurancejournal.com/news/national/2015/10/21/385672.htm. This breach arose in connection with Sony's release of the movie, *The Interview*, which was a comedy set in North Korea. *Id.*

a layer of incentive to bolster cybersecurity. There are problems, however, with relying on tort law. First, if damages are at issue, it means the harm has already occurred. Tort law may compensate victims after harm has occurred, but it may not sufficiently incentivize the development of preventative measures. Second, tort law does not solve the problem of negative externalities. If an electric utility has weak cyberdefenses and is breached, not all persons affected by the power loss will be able to prove proximate causation. Thus, the utility will not bear all the loss caused by its inadequate cyberdefenses. Finally, the country may not want to rely on the tort system to prevent catastrophic attacks.

Thus, the question remains whether current law results in adequate cybersecurity. Given the numerous issues involved, a voluntary approach may be the most prudent, least disruptive course to take. However, there are obvious problems with this approach.

IV
THE DISADVANTAGES TO A VOLUNTARY APPROACH TO PROTECTION OF CI

Widely accepted economic theory tells us that the free market will result in an undersupply of public goods. There are two reasons for the significant underinvestment in cybersecurity protection of CI. Because private businesses are profit driven, they will produce only those goods from which they can earn a profit. As a result, they will not produce public goods because public goods are nonexcludable.[121] In other words, the positive externalities enjoyed by third parties generated by investment in cybersecurity cannot be captured as profit by the provider of the cybersecurity. A supplier of a public good (like cybersecurity of CI) cannot exclude free riders or force them to pay.[122] A free market is unable to provide a profit incentive for the production or supply of public goods. The other side of this coin is that entities that own CI do not bear the full cost of an underinvestment in cybersecurity because much of the cost will be borne by unrelated third parties. Even self-interest in self-protection does not provide adequate economic incentives in the case of protection of CI. An electric utility may calculate that in the event of a cyberattack that destroys power generation equipment, it will incur a certain cost to repair the damage. However, the cost of repair does not

121 *See Public Goods Podcast, supra* note 64.

122 *Id.*

capture the external costs to all the customers who suffer from a power outage. For these reasons, there will likely be underinvestment in cybersecurity:[123]

"Many companies that operate critical infrastructure tend to underinvest in cyber-defense because of negative externalities, positive externalities, free riding, and public goods problems—the same sorts of challenges the modern administrative state encounters in a variety of other contexts."[124]

The market, by itself, is unable to provide sufficient incentives for an optimal amount of spending on cybersecurity. A report by a leading consulting firm seems to confirm this conclusion. According to the report, global cybersecurity spending was expected to reach an all-time high of $76.9 billion in 2015.[125] However, the majority of IT executives anticipated receiving only half of the funding necessary to execute their preferred security strategies.[126] The report highlighted the problem of this underfunding. It went on to state that U.S. businesses encounter approximately 1.7 successful cyberattacks per week and incur annual costs of $12.7 million per business to address the impacts.[127] The frequency, complexity, and costs associated with

---

[123] Sales observes,

> If this analysis is correct, then strategically significant firms in uncompetitive markets are less likely to adequately invest in cyber-security than ordinary firms in competitive markets. The question then becomes who should be responsible for securing these most sensitive companies against the most dangerous adversaries. Economists often argue that risk should be allocated to the low cost avoider. If the government can reduce a vulnerability more efficiently than a firm, it should pay; if the firm can reduce a vulnerability more efficiently, it should pay. But there is no single low cost avoider in this context. Defending critical infrastructure against sophisticated cyber-attackers is a task that features dueling comparative advantages. Private firms typically know more than outsiders, including the government, about the architecture of their systems, so they often are in a better position to know about weaknesses that intruders might exploit. The private sector thus has a comparative advantage at identifying cyber-vulnerabilities. On the other hand, the government's highly skilled intelligence agencies typically know more than the private sector about malware used by foreign governments and about how to defeat it. The government thus has a comparative advantage at detecting sophisticated attacks and developing countermeasures. This suggests that responsibility for defending the most sensitive systems against the most sophisticated adversaries should be shared.

Sales, *supra* note 12, at 1517–18.

[124] *Id.* at 1507.

[125] BOOZ ALLEN HAMILTON, CYBER ROI: A PRACTICAL APPROACH TO QUANTIFYING THE FINANCIAL BENEFITS OF CYBERSECURITY 1 (2015).

[126] *Id.*

[127] *Id.*

attacks are increasing, but the report concludes that many organizations are reluctant to increase cybersecurity spending because they are unable to accurately quantify the financial value of prospective investments.[128]

The problem is compounded by the vulnerabilities of smaller companies that are linked to a larger company. Returning to the example of the Boeing 777 from this Article's introduction, even if it is assumed that Boeing correctly assessed the risk to its systems and invested the right amount in cybersecurity defense, the same may not be true for the hundreds of suppliers who supply the parts that go into the aircraft. For example, suppose a small company provides parts for the in-flight entertainment system and assume that the parts are accessible to the Internet. Does that small supplier have sufficient incentive to invest properly in cybersecurity when the monetary damage to it of a cyberattack on its parts is tiny compared to the possible harm that may occur if the safety of the aircraft is breached by an attack through the in-flight entertainment system? Does a small supplier have the money to invest in increased cybersecurity? Boeing may have a large budget to devote to it, but what about the hundreds of smaller companies in the supply chain? [129]

The financial costs faced by small vendors to larger businesses is exemplified by the challenges that threaten law firms. Law firms are part of CI systems because they are linked to clients who operate CI. The owners and operators of CI systems are vulnerable to threats and breaches initiated through attacks on their law firms.[130] The

---

128 *Id.*

129 *See* Shackelford & Russell, *Above the Cloud*, *supra* note 47, at 641 (discussing this hypothetical threat).

> The proverbial "weak link" in the chain of CI could result in catastrophic economic damage, which is compounded by the sheer number of access points that cyber attackers may exploit. Government contractors, private-sector actors, public-sector organizations, utilities companies, and so on, all have separate regulators, differing cybersecurity standards, and long supply chains.

Id. The use of everyday, seemingly innocuous devices to cripple the Internet has already happened. In October 2016, there was a massive distributed denial of service attack that shut down major websites. Hackers used hundreds of thousands of web-connected devices such as webcams and DVRs to launch the cyberattack. *See* Sam Thielman & Elle Hunt, *Cyber Attack: Hackers 'Weaponised' Everyday Devices with Malware*, GUARDIAN (Oct. 22, 2016, 1:47 AM), https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault.

130 *See* Julie Sobowale, *Large or Small, Law Firms are Learning They Must Deal with Cybersecurity*, 103 A.B.A. J. 34, 36 (2017). Law firms have suffered theft of money from their bank accounts, theft of confidential client information for use in illegal trading, and

vulnerabilities are widely acknowledged, but the response has been slow due to the high financial cost of improving cybersecurity defenses.[131] The simple but necessary step of upgrading software poses a financial problem for many firms, and this cost generally cannot be passed on to clients.[132] Law firms are a typical provider or supplier to the larger businesses that own CI systems, and there is no reason to think that the financial problems for law firms are unique to them. Thus, studies in these areas produce expected findings.

> The studies found that many firms regard cyber-security as little more than "a last box they have to check," and that they neglect network security because they find it too expensive. In particular, McAfee [a provider of cybersecurity software] found that companies often have weak authentication requirements–tools that can verify that the person who is accessing a system is who he says he is, and is authorized to access the system. Even fewer have systems that can monitor network activity and identify anomalies. Other studies reveal that some companies' defenses are so poor they don't even know when they've suffered an attack.[133]

Cybersecurity for CI relies on financial investments by private parties in their systems. Even assuming that all private parties understand the importance of cybersecurity, they may not have the money to spend on it.[134]

V
A MODEST PROPOSAL TO BOLSTER CYBERSECURITY DEFENSES

The traditional approach to increasing public goods such as cybersecurity is well known. The government can play its traditional role as the provider or facilitator.[135] The government has a unique role because it does not face the same problems as private businesses that need a profit incentive.[136] The government has taken the first

---

disclosure of confidential documents in the notorious Panama Papers incident, all through cyberattacks. *Id.* at 40–41.

131 *Id.* at 36.

132 *Id.*

133 Sales, *supra* note 12, at 1512.

134 *See* Tran, *supra* note 106, at 483, 486.

135 "So how do we get public goods? The government steps in. Unlike a private firm, the government has no profit motive. And the government reduces the free rider problem by collecting taxes from consumers to help fund public goods." *Public Goods Podcast*, *supra* note 64.

136 Frischmann's article states,

> In other words, it is generally accepted that the market will fail in one way or another to efficiently provide society with infrastructure and that there is some

steps of creating a voluntary framework. However, there is more that can be done. To this end, this Article proposes a modest, incremental expansion of the government's role that builds on the voluntary framework. The continued interaction between the private and public sectors remains crucial because each has its own areas of advantages the other side lacks.

A significant barrier to improvement in cybersecurity is the cost, and cost is likely to be a more challenging issue for smaller firms.[137] To address this problem, the federal government could subsidize, in whole or part, upgrades to cybersecurity defenses.[138] Government subsidization is a traditional response to encourage the production of public goods.[139] The appeal of subsidies in this particular area is that the federal government already subsidizes protection of CI. The proposal is to simply expand subsidies already authorized by Congress to include more private entities.

Federal legislation to encourage private-sector protection of CI systems is already in place. For example, Title 10 of the United States Code includes the following provision:

> role for government intervention . . . . The question then becomes one of comparative institutional analysis: how should the government modify or regulate the market?

Frischmann, *supra* note 60, at 940. He adds, "[c]ritically, many infrastructure resources act as inputs into a wide variance of socially valuable activities, including the production of public goods and nonmarket goods. These activities generate significant social welfare gains that are generally associated with traditional infrastructure, yet underappreciated with respect to nontraditional infrastructure." *Id.* at 932.

137 *See* Robert Gyenes, Note, *A Voluntary Cybersecurity Framework is Unworkable—Government Must Crack the Whip*, 14 U. PITT. J. TECH. L. & POL'Y 293, 295 (2014) (claiming that voluntary policy "creates a financial burden on the target 'critical' infrastructure without providing a solution"). "In part because the government doesn't provide any funding, businesses have decided not to invest in new secure facilities and network upgrades to handle classified data." *Id.* at 305. "Under the current Framework, companies are left to wonder how they will finance any voluntary cyber improvements without incentives. Corporations failing to invest in cybersecurity often cite budget constraints as 'the number one challenge to contributing to the [cybersecurity] levels the business expects.'" *Id.* at 311.

138 *See* Goldsmith, *supra* note 112 (explaining that subsidies may be considered as one of many forms of government regulation).

> Regulation can serve the public interest in two ways. First, it can address "market failure" or the absence of one or more of the factors necessary for an efficient market. A private market is "efficient" when it produces only those goods and services most desired by consumers. Second, regulation is justified on the ground that the outcome of markets is inconsistent with important collective social values other than economic efficiency.

PIERCE, JR. ET AL., *supra* note 75, at 13–14.

139 *See* Sales, *supra* note 12, at 1519.

> In order to meet the national security objectives in section 2501(a) of this title, the Secretary of Defense shall establish a program under which the Secretary may issue guarantees assuring lenders against losses of principal or interest, or both principal and interest, for loans made to qualified commercial firms to fund, in whole or in part, any of the following activities:
> (1) The improvement of the protection of the critical infrastructure of the commercial firms.
> (2) The refinancing of improvements previously made to the protection of critical infrastructure of the commercial firms.[140]

The necessity for this statute was spurred by national defense issues, and this Article referenced the DOD's interim final rule requiring contractors to meet certain NIST standards. In responding to that rule, the Small Business Administration (SBA) raised the issue of the financial burdens faced by small businesses in upgrading cybersecurity. To ease the burden, the SBA recommended "that DOD consider alternatives, such as collaborating with universities or other organizations to provide low-cost cybersecurity services to small businesses, or providing a one-time subsidy to small businesses to help cover the cost of initial consultations with third-party vendors."[141]

This Article proposes the expansion of subsidies beyond matters under the jurisdiction of the DOD so that other CI systems receive government support. The fact that Congress and the DOD already have a subsidy program in place for CI should be viewed as strong support for the case in favor of subsidies and is a clear indication that Congress recognizes the need for such financial support for the private sector. A main problem seems to be that such programs are not available for all CI systems.

CONCLUSION

This Article's proposal depends on federal budget issues and political will.[142] However, if the country is to maintain a voluntary

---

[140] 10 U.S.C. § 2541(a) (2012).

[141] *See* SBA, Opinion Letter on Interim Rule, Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (Feb. 29, 2016), https://www.sba.gov/sites/default/files/DFARS_security_interim_comment_letter.pdf.

[142] This Article focuses on economic problems in the form of market failure as obstacles to optimal protection of CI. However, a more complete discussion requires acknowledgement of the political obstacles as well. Some powerful businesses in the private sector oppose government efforts to strengthen cybersecurity defenses and spend millions of dollars in lobbying efforts to resist such efforts. *See* CLARKE & KNAKE, *supra*

approach to cybersecurity, it seems any improved approach will necessarily include expanded subsidization to assist the private sector. The government's existing legislation acknowledges the merits of subsidies for CI. Because the use of subsidies to protect CI already has congressional approval in some instances, an increase in the role of subsidies deserves further consideration. In enacting the Critical Infrastructures Protection Act of 2001, Congress found that "[p]rivate business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors."[143] In order to ensure full and optimal participation by the private sector, some sort of government support is necessary. Otherwise, the public good nature of cybersecurity of CI will continue to frustrate optimal protection.

Government support is especially vital because the cybersecurity battle changes constantly. As soon as one threat is addressed, another replaces it. Defense requires constant monitoring and response, and the cost to the private sector is significant. Experts in the area know the nature of the problems. However, the problems are extremely difficult to quantify. How much is the right amount of spending on cybersecurity? What is the likelihood of any particular kind of attack, and what is the estimated amount of resulting damage? How does one go about determining numbers like this? Private businesses cannot afford to overspend on a low-risk problem, but they also expose themselves if they underspend on a high-risk problem. Additionally,

---

note 37, at 137–43 (discussing Microsoft's lobbying efforts). In addition to the influence of money on the political process, politicians themselves may also be obstacles. This is Clarke's description of the situation:

> Congress is a federation of fiefdoms, subject to the vicissitudes of constant fund raising and the lobbying of those who have donated the funds. That situation has two adverse consequences with regard to congressional involvement in cyber war oversight. First, everyone wants his or her own fiefdom. Congress has resisted any suggestion, such as was made by Senator Bob Bennett (Republican of Utah), that there be one committee authorized to examine cyber security . . . . Second, Congress 'eschews regulation' and spits it out. The influential donors from the information technology, electric power, pipeline, and telecommunications industries have made the idea of serious cyber security regulations as remote as public financing of congressional campaigns or meaningful limits on campaign contributions.

Id. at 263. Of course, this is one person's personal opinion. Yet, it is an opinion that deserves consideration.

[143] 42 U.S.C. § 5195c(b)(2) (2012).

private businesses may not be positioned to be able to assess the risk or likelihood of an attack. A proposal for increased subsidization is a mild response to the nature of the problem. However, if there was a better solution, it would probably already be in place. At a minimum, the goal of this Article is to increase awareness of the problems and the threat potentials, as reliance on the Internet continues to grow.