VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2014 UNIVERSITY OF VIRGINIA VOL. 18, NO. 03

Critical Infrastructure: Legislative Factors for Preventing a "Cyber–Pearl Harbor"

ROBERT KENNETH PALMER†

† Assistant Professor, United States Air Force Academy, LL.M., The George Washington University Law School; J.D., Marquette University Law School; B.A., University of Minnesota, Duluth. Major Robert K. Palmer thanks his thesis advisor, Professor Gregory E. Maggs, for the excellent feedback and guidance, and his wonderful family, without whose support he could not have undertaken this article in the first place.

Major Robert K. Palmer serves in the U.S. Air Force Judge Advocate General's Corps. This paper was submitted in partial satisfaction of the requirements for the degree of Master of Laws in National Security and Foreign Relations at The George Washington University Law School. The views expressed in this paper are solely those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or U.S. Government.

ABSTRACT

Warnings about the possibility of a "cyber–Pearl Harbor" attack on our nation's vulnerable critical infrastructure have been promulgated with increased frequency over the past several years. This Article proposes two essential baseline factors for cyber-legislation to incorporate in order to protect the nation's critical infrastructure: (1) centralized and mandatory threat communication that is carefully tailored, and (2) government-incentivized, but private industry–led, security development. This Article arrives at these conclusions by first examining the currently existing cyber-threat to critical infrastructure through several examples before laying out why critical infrastructure has proven so vulnerable to, and unprepared for, cyber-attacks. Then, this Article analyzes how several legislative proposals can be utilized to address the vulnerability factors identified and why current law and executive action falls short of effective cybersecurity.

TABLE OF CONTENTS

I. INTRODUCTION

On October 11, 2012, then–Defense Secretary Leon Panetta warned that the United States risked facing a "cyber–Pearl Harbor" attack from aggressor nations or extremist groups who would use cyber-tools to attack U.S. critical infrastructure networks.[1] The aggressors can launch attacks with cyber-tools to gain control of our nation's critical infrastructure and derail passenger trains, contaminate water supplies, shutdown the power grid or even a combination of coordinated such attacks, causing physical destruction and loss of life on a scale that "would paralyze and shock the nation."[2] Defense officials insisted that Secretary Panetta's comments were by no means aggrandizement but rather that he was responding to a real and recent wave of cyber-attacks and that he was seeking legislation to require new standards for critical infrastructure facilities where a computer breach could cause significant casualties or economic damage.[3]

Cyber-attacks on U.S. supplies and distribution of water and electricity, banking, communications, transportation and other systems vital to the everyday operation of our government, economy and well-being, what is generally known

---

[1] Leon E. Panetta, U.S. Sec'y of Defense, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), *available at* http://defense.gov/Transcripts/Transcript.aspx?TranscriptID=5136.

[2] *Id.*

[3] Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES, Oct. 11, 2012, *available at* http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

as critical infrastructure, is not a new phenomenon.[4] Critical infrastructure includes a diverse and vast variety of assets, including not only energy, water and transportation, but also assets like banking and finance, agriculture, emergency services, communications, and chemicals, among others.[5] Although assets like water are owned and operated by governmental or quasi-governmental entities, the vast majority of these assets are in private hands.[6] Unlike military or intelligence networks, which are defended and overseen by the Department of Defense (DoD), or various civilian government networks, which are defended and overseen by the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Office of Budget and Management, no one entity defends the private networks that most critical infrastructure relies upon.[7] Rather, the policy

---

[4] *See generally* 42 U.S.C. § 5195(e) (2012) (defining specifically critical infrastructure as "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").

[5] *See* U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 19, Table S-1 (2009) [hereinafter NATIONAL INFRASTRUCTURE PROTECTION PLAN], *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (dividing critical infrastructure into eighteen sectors, including: agriculture and food, defense industrial base, energy, healthcare and public health, national monuments and icons, banking and finance, water, chemical, commercial facilities, critical manufacturing, dams, emergency services, nuclear reactors, materials and waste, information technology, communications, postal and shipping, transportation systems and government facilities).

[6] *Id.* at 11.

[7] JAMES R. LANGEVIN ET AL., CTR. FOR STRATEGIC & INT'L STUDIES (CSIS), A REPORT OF THE CSIS COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY: CYBERSECURITY TWO YEARS LATER 7 (2011), *available at*

regarding private critical infrastructure networks has been to rely on individual action by the owners and operators and faith in market forces to drive security improvements.[8]

Secretary Panetta's warning of a "cyber–Pearl Harbor" attack by our enemies on these resources does not constitute new recognition of this vulnerability from a government perspective; the analogy has been in use by government officials going back to at least the mid-1990s and with increasing frequency since the 9/11 terrorist attacks.[9] The Presidential Decision Directive 63 (PDD-63) in 1998 acknowledged that increasingly automated and interlinked critical infrastructure systems to the Internet and larger networks due to technological advances and efficiency improvement was resulting in its growing vulnerability to cyber-attack.[10] The PDD-63 further stated that because the U.S. possessed the world's strongest military and largest economy, future enemies could harm us in non-traditional ways by instead attacking these vulnerable systems that our national power is reliant upon.[11] In response, the PDD-63 stated that the U.S. would "take all necessary measures to

---

http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

[8] *Id.*

[9] *See generally* David Perera, *Stop Saying "Cyber Pearl Harbor"*, FIERCEGOVERNMENTIT (Jun. 13, 2012) http://www.fiercegovernmentit.com/story/stop-saying-cyber-pearl-harbor/2012-06-13 (compiling the chronological use of the "cyber–Pearl Harbor" analogy by U.S. government officials).

[10] PRESIDENTIAL DECISION DIRECTIVE NSC-63, CRITICAL INFRASTRUCTURE PROTECTION 2 (1998) [hereinafter PDD-63], *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf.

[11] *Id.* at 1–2.

swiftly eliminate any significant vulnerability to . . . cyber-attacks on our critical infrastructure."[12]

In the fifteen years since the PDD-63, there have been subsequent and significant published presidential decrees on the growing vulnerability of the nation's critical infrastructure to enemy attack and similar calls for elimination of those vulnerabilities.[13] Yet, given Secretary Panetta's comments, the nation presently remains vulnerable to a "cyber–Pearl Harbor" event and evidence continues to mount that the nation's adversaries continue to probe and explore this avenue of attack against us. President Obama even acknowledged critical infrastructure cyber-vulnerabilities in his 2013 State of the Union address, stating: "[O]ur enemies are also seeking the ability to sabotage our power grid, our financial institutions . . . . We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[14] Additionally, the President, like Secretary Panetta, was emphatic that legislation from Congress was necessary to secure our networks and deter attacks.[15]

---

[12] *Id.* at 2.

[13] *See, e.g.*, U.S. Computer Emergency Readiness Team (US-CERT), *National Strategy to Secure Cyberspace* (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf; US-CERT, *Homeland Security Presidential Directive 7* (2003), *available at* http://www.dhs.gov/homeland-security-presidential-directive-7 - 1; US-CERT, *Comprehensive National Cybersecurity Initiative* (2008), *available at* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[14] Barack Obama, U.S. President, Remarks by the President in the State of the Union Address (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

[15] *Id.*

Congress has not been entirely idle on the issue, but despite several significant and competing proposals on how to address cybersecurity for critical infrastructure, none have yet become law.[16] A major impediment to the enactment of legislation in this area has been a debate on whether government should mandate minimum security standards and threat communication or merely encourage information sharing and security improvement in private sector critical infrastructure.[17] Those who generally favor mandating minimum standards believe that voluntary efforts and market forces cannot deliver adequate security in a reasonable period to protect the U.S. from the very real threats they perceive rapidly mounting against critical infrastructure.[18] Alternatively, those who oppose government mandates, particularly those in the critical infrastructure industry, believe the government

---

[16] *E.g.*, Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, S. 3342, 112th Cong. (2d Sess. 2012) [hereinafter SECURE IT]; Cybersecurity Act of 2012, S. 3414, 112th Cong. (2d Sess. 2012); Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2d Sess. 2011) [hereinafter CISPA].

[17] *See* Ed O'Keefe & Ellen Nakashima, *Cybersecurity Bill Fails in Senate*, WASH. POST, Aug. 2, 2012, *available at* http://articles.washingtonpost.com/2012-08-02/world/35493132_1_cybersecurity-bill-jay-carney-house-lawmakers; *see also* Tom Gjelten, *Bill Would Have Businesses Foot Cost of Cyberwar*, NPR (May 8, 2012, 9:52 AM), http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war; Tom Gjelten, *Cybersecurity Bills Compete for Attention*, NPR (Apr. 16, 2012, 3:00 PM), http://www.npr.org/2012/04/16/150745384/cybersecurity-bills-compete-for-attention.

[18] *E.g.*, LANGEVIN ET AL., *supra* note 7, at 7; Joseph I. Lieberman & Susan Collins, *At Dawn We Sleep*, N.Y. TIMES, Dec. 6, 2012, *available at* http://www.nytimes.com/2012/12/07/opinion/will-congress-act-to-protect-against-a-catastrophic-cyberattack.html?_r=0.

lacks the understanding to regulate effectively across so many diverse sectors and believe mandates will impose high costs that will stifle market place innovation, ultimately leaving the nation even less secure.[19]

This Article proposes two essential baseline factors for cyber-legislation to incorporate in protecting the nation's critical infrastructure: (1) centralized and mandatory threat communication that is carefully tailored, and (2) government-incentivized, but private industry–led security development. This author does not suggest that these factors alone will result in immunization of critical infrastructure from cyber-attack. Rather, this author suggests that these two factors are essential foundational elements upon which will result in a model of strengthened cybersecurity that can be developed for critical infrastructure going forward.

Regarding the first factor, centralized and mandatory threat communication that is carefully tailored, this Article proposes that continuation of the current ad hoc, piecemeal, and voluntary sharing scheme between and amongst the government and private industry is not likely to achieve any significant protection against cyber-attacks. There are simply too many perceived legal and business disincentives from the industry standpoint for the private industry to voluntarily share threat information with each other and/or the government in an effective manner. Rather, centralized and some mandatory

---

[19] STEWART BAKER ET AL., IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 28–29 (2009), *available at* https://www.dsci.in/sites/default/files/NA_CIP_RPT_REG_2840.pdf (surveying critical infrastructure executives who expressed the attitude that regulation would "flatten" standards, which although might improve security for some, would set a floor which more sophisticated enterprises could otherwise easily exceed but would have less or no incentive to do so).

threat communication would ensure that vital cyber-threat information is in fact shared with those that can make use of it in a timely manner. This Article also proposes that the creation of a nongovernmental, nonprofit clearinghouse would be best situated to act as a one-stop focal point for government and private industry sharing, because it could remain unburdened by the drawbacks of an industry- or government-centric sharing portals. Additionally, legal obstacles to information sharing are not insurmountable. Careful tailoring and defining of what information is actually shared can avoid any feared overreaching or abuse by the government and/or industry and can avoid undermining important antitrust or privacy laws. Finally, liability protections could be instituted to protect corporate interests.

In regards to the second factor, government-incentivized, but private industry–led, security development, this Article proposes that the dynamic world of cyber threats requires nimble and innovative industry specific expertise in each affected industry area to develop effective security standards. Rather than using a cumbersome and time-consuming rule-making process to draft standards, the government should focus on creating strong incentives to motivate companies to adopt effective security practices and invest in the substantial technology necessary to make stronger cybersecurity possible. Incentives could include various forms of liability protection, research and development grants, and tax incentives for those that adopt the industry standards and invest in security technology.

Part II of this Article examines the current cyber-threat to critical infrastructure. Several examples of cyber-attacks on critical infrastructure will be detailed in order to demonstrate its current capability. Part III explores why critical infrastructure has proven so vulnerable to and unprepared for

cyber-attacks. Specifically, weak information sharing between and amongst the government and private industry, on top of the industrial control system (ICS) not being designed for an era of ever increasing network and Internet connectivity, have many of the most serious problems that plague critical infrastructure. Part IV proposes and analyzes how already proposed different legislative possibilities can be used to address the vulnerability factors identified. Included is a discussion of why an executive order already issued in this area is an insufficient answer.

II. U.S. CRITICAL INFRASTRUCTURE UNDER ATTACK

A 2009 Forbes article rendered what an attack on critical infrastructure might look like from the perspective of an everyday citizen:

> First your cell phone doesn't work. Then you notice that you can't access the Internet. Down the street, ATMs won't dispense money. Traffic lights don't function, and calls to 911 don't get routed to emergency responders. Radios report that systems controlling dams, railroads and nuclear power plants have been remotely infiltrated and compromised. The air-traffic control system shuts down, leaving thousands of passengers stranded or rerouted and unable to communicate with loved ones. This is followed by a blackout that lasts not hours but days and even weeks. Our digital civilization shudders to a halt. When we emerge, millions of Americans'

> data are missing, along with billions of dollars.[20]

But is this just the simple hyperbole of an outsized Hollywood imagination? This Part examines the threat to critical infrastructure through several examples of real-world cyber-attacks and the likelihood that more attacks will follow.

A. The AURORA Experiment

In March of 2007, the Idaho National Laboratory set up an experiment to see whether it was possible to sabotage and blow up a twenty-seven ton electricity generator using only a keyboard, mouse, and the Internet.[21] The experiment was called AURORA.[22] What the scientists found was that even though they were miles away, they were able to bypass security, hack into and take control of the generator, and by opening and closing breakers within the machine, were able to cause the machine to tear itself apart, catch fire, and eventually explode, all the while making the operator's screen appear as if the machine was operating perfectly normal.[23]

The videotape of the attack demonstrated not only the leap from theory to reality but also that the subsequent fallout of a big generator like the one used Aurora would likely have

---

[20] John P. Avlon, *The Growing Cyberthreat*, FORBES (Oct. 20, 2009, 1:49 PM), http://www.forbes.com/2009/10/20/digital-warfare-cybersecurity-opinions-contributors-john-p-avlon.html.
[21] JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 93 (Penguin Press 2011); *60 Minutes: Cyber War* (CBS television broadcast June 13, 2010), *available at* http://www.cbsnews.com/videos/cyber-war.
[22] BRENNER, *supra* note 21, at 93.
[23] *Id.* at 93–94; *60 Minutes: Cyber War*, *supra* note 21.

effects far beyond the kinetic explosion and immediate loss of electricity to an area.[24] These generators are expensive, made outside the U.S., and thus require an order lead time of a few months to replace; a well-planned attack can take a power plant offline effectively for months.[25] Multiple attacks on power plants might even blackout entire regions.[26]

B. A Theory No Longer

Since the AURORA experiment in 2007, the U.S. has moved beyond the theoretical and into an era where cyber-attacks on the critical industry are actually occurring and in an increasing number against a wide variety of targets. In sum, 198 cyber-incidents against critical infrastructure were reported to the Department of Homeland Security in 2011, which was a 2100 percent increase from the nine reported in 2009.[27] It is also increasingly clear that various U.S. enemies are taking an interest in this line of attack.

Around the entire country, the Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control critical infrastructure systems, similar to the systems that controlled the AURORA generator and provide early warning of system failures that could lead to disasters.[28] Many

---

[24] *60 Minutes*, *supra* note 21.

[25] *Id.*

[26] *Id.*

[27] U.S. DEP'T OF HOMELAND SEC., ICS-CERT MONITOR 10 (2012), *available at* http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf; U.S. DEP'T OF HOMELAND SEC., ICS-CERT MONITOR (2011), *available at* http://ics-cert.us-cert.gov/monitors/ICS-MM201112 (using fiscal year time reporting, which comprises the time period from October 1 to September 30).

[28] NAT'L COMMC'NS SYS., TECHNICAL INFORMATION BULLETIN 04-1, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

are now networked to, and controlled via, the Internet to boost efficiency by allowing workers to operate equipment remotely, but this also opens a doorway through which cyber-attacks may infiltrate.[29] Computers seized from al-Qaeda have been found to contain details about American SCADA systems that control electrical grids, oil and gas pipelines, water storage, and distribution facilities and other systems.[30] One set of computers even contained schematics of a U.S. dam and control system engineering software that enabled them to simulate the effects of catastrophic flooding.[31]

Terrorists are by no means the only groups interested in exploiting American critical infrastructure vulnerabilities. The "Comment Crew", a sophisticated Chinese hacking group that is part of the People's Liberation Army, has increasingly turned its focus from simple corporate espionage and intellectual property theft to infiltration of the private companies involved in U.S. critical infrastructure.[32] In one particular case, staff at Digital Bond, a firm that specializes in industrial-control computers, received phishing e-mails subsequently traced to the Comment Crew.[33] The e-mails contained a link with a

---

(2004), *available at* http://scadahacker.com/library/Documents/ICS_Basics/SCADA Basics - NCS TIB 04-1.pdf.

[29] BRENNER, *supra* note 21, at 97.

[30] Avlon, *supra* note 20.

[31] *Id.*

[32] David E. Sanger et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 18, 2013, *available at* http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all.

[33] Kim Zetter, *Maker of Smart-Grid Control Software Hacked*, WIRED, Sept. 26, 2012, *available at* http://www.wired.com/2012/09/scada-vendor-telvent-hacked.

hidden malware tool that would have given them control of the recipients' computers and potentially given them access to confidential client information, including a major water project and power plant the company was consulting on.[34]

Even more troubling was a similar but successful attack on Telvent, a company that specializes in designing ICS, where through its customers, detailed blueprints and remote access to the valves, switches and security systems of more than 60 percent of North American oil and gas pipelines were obtained.[35] Telvent subsequently terminated its remote access to its customers' systems to protect the customers from potential intrusion and takeover, but the hackers made away with highly specialized software that is heavily used in running the controls systems for North American oil and gas pipelines as well as some water system networks.[36] That stolen software code could be the source for future attacks if it is dissected and scoured for "zero-day"[37] vulnerabilities that can be exploited for attacks on the control systems that also use the software.[38] Against such malware attacks that take advantage of those vulnerabilities, protection such as firewalls and intrusion detection systems would be virtually worthless.[39]

---

[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *See* JEFFREY CARR, INSIDE CYBER WARFARE 152 (2d ed., 2011) (defining a "zero-day" exploit as when vulnerabilities are exploited before, or on the same day as, the vulnerability is learned about).
[38] *See* Zetter, *supra* note 33.
[39] *See* ARIEL FUTORANSKY ET AL., SIMULATING CYBER-ATTACKS FOR FUN AND PROFIT, *available at* http://www.coresecurity.com/files/attachments/SimulatingCyberAttacks.pdf .

Cyber-attacks on other SCADA systems, such as municipal water systems, have not required the sophistication of "zero-day" exploits to be successful. These attacks do not necessarily require the funding, manpower, or resources of foreign governments or terrorist organizations. An unidentified "hacktivist"[40] using the alias "pr0f" hacked into a suburban Houston waste-water treatment plant and later posted screenshots of his ability to view and manipulate the control systems as proof of his intrusion.[41] The hacker stated that he was not a security professional and did not work in the SCADA sector but rather had simply read a few basic books on ICS.[42] The hacker also stated in an e-mail that he got into the system through "a combination of poor configuration of services, bad password choice, and no restrictions on who can access the interfaces" and that his intent was to try and force the U.S. government to acknowledge how easy it was to hack into and control these systems.[43] A control systems presentation at the DHS's Working Group ("ICSJWG") predicted that such a cyber-attack on a water plant can be used to disable the water distribution system altogether, interfere

---

[40] *See* FRANÇOIS PAGET, MCAFEE LABS, HACKTIVISM: CYBERSPACE HAS BECOME THE NEW MEDIUM FOR POLITICAL VOICES 3 (2010), *available at* http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf (defining "hacktivists" as a merger of hacker and activist, where groups or individuals infiltrate networks and commit cyber-attacks for economic, political, or religious interests).

[41] Elinor Mills, *Hacker Says He Broke into Texas Water Plant, Others*, CNET (Nov. 18, 2011, 3:35 PM), http://news.cnet.com/8301-27080_3-57327968-245/hacker-says-he-broke-into-texas-water-plant-others.

[42] *Id.*

[43] *Id.*

with the treatment equipment to cause chemical under or over-dosing, or even hold the system for ransom.[44]

Other sectors of critical infrastructure in the U.S. have also been targeted. In September of 2012, a post alleged to be authored by an Iranian-sponsored Islamist group, Izz ad-Din al-Qassam Cyber Fighters, announced that they would launch a major directed denial-of-service (DDoS) attack against the largest U.S. banks.[45] Approximately two weeks later, the worst DDoS attack in history occurred, preventing customers from accessing the websites of some of the nation's largest banks such as Chase, Bank of America, Wells Fargo, and U.S. Bank, among others.[46] The unprecedented scale and effectiveness of the attacks was attributed to the attackers' engineering of multiple networks of computers in data centers around the

---

[44] John McNabb, Address at the ICSJWG 2012 Spring Conference: Protection of Control Systems at Drinking Water Utilities 15 (May 9, 2012), *available at* http://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/S2012/D22pmTr3_McNabb _ProtectCS- DrinkWaterUtil_p.pdf (slideshow of the presentation).

[45] David Goldman, *Major Banks Hit with Biggest Cyberattacks in History*, CNNMONEY (Sept. 28, 2012, 9:27 AM), http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html; *see also* Mindi McDowell, *SECURITY TIP (ST04-015): Understanding Denial of Service Attacks*, US-CERT (last revised Feb. 6, 2013), https://www.us-cert.gov/ncas/tips/ST04-015 (stating that denial-of-service (DoS) attacks occur when an attacker "floods" a network with information, thus overloading a server's ability to process requests and denying access to the website, but distributed DoS attacks, in contrast, occur when an attacker takes advantage of security vulnerabilities or weaknesses in multiple "innocent" computers to take control of them and simultaneously launch multiple DoS attacks at one time).

[46] David Goldman, *Massive Bank Cyberattack Planned*, CNNMONEY (Dec. 13, 2012, 4:02 PM), http://money.cnn.com/2012/12/13/technology/security/bank-cyberattack-blitzkrieg/index.html.

world, transforming the normal online DDoS attack equivalent of a "few yapping Chihuahuas into a pack of fire-breathing Godzillas."[47] Neither the customers nor the banks themselves were able to conduct business online for various periods of time.[48]

However, some banks took the early warning seriously and thus, were the least affected with only intermittent access problems.[49] Other banks were not prepared and experienced outages that lasted as long as a day.[50] This was the case in spite of the fact that the Financial Services and Information Sharing and Analysis Center (FS-ISAC) has been operating since 1999, which is specifically tasked with cybersecurity and cyber-threat information sharing among financial service providers.[51] Membership by banks in the FS-ISAC is voluntary by paid subscription, and it receives threat information from its subscribers on a voluntary, and even anonymous, basis.[52] Although very specific banks were threatened by the Izz ad-

---

[47] Nicole Perlroth & Quentin Hardy, *Bank Hacking was the Work of Iranians, Officials Say*, N.Y. TIMES, January 8, 2013, *available at* http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0.

[48] Chris Strohm & Eric Engleman, *Cyber Attacks on U.S. Banks Expose Computer Vulnerability*, BLOOMBERG BUS. WK. (Sept. 27, 2012), http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability.

[49] Goldman, *supra* note 46.

[50] *Id.*

[51] *About FS-ISAC*, FINANCIAL SERVICES AND INFORMATION SHARING AND ANALYSIS CENTER, https://www.fsisac.com/about (last visited Aug. 17, 2014).

[52] FINANCIAL SERVICES AND INFORMATION SHARING AND ANALYSIS CENTER, OPERATING RULES 14–16 (2012), *available at* https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2012.pdf.

Din al-Qassam Cyber Fighters on September 18th, the day the attacks began, FS-ISAC only raised its alert level and warned its members on September 19th, the following day.[53]

The fact that the hackers in this instance broadcasted their intentions and targets and the banks were still unable to sufficiently protect themselves demonstrates that the financial industry and the U.S. government are still struggling to manage fast-moving network threats.[54] Sustained and recurrent DDoS attacks against the banking infrastructure could result in shaken consumer confidence and a loss of faith in the banking industry, which can serve to destabilize or undermine the industry completely.[55]

There is perhaps no better example of a real world cyber-threat to critical infrastructure than that presented by the Stuxnet worm attack on Iran's nuclear program. While not an attack on U.S. critical infrastructure, the Stuxnet was specifically developed to seek out and disrupt a particular ICS found in many different critical infrastructure facilities.[56] The sophisticated worm, likely developed by the U.S. and Israel,

---

[53] Nicole Perlroth, *Attacks on 6 Banks Frustrate Customers*, N.Y. TIMES, Sept. 30, 2012, *available at* http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html (stating that posts from the Izz ad-Din al-Qassam Cyber Fighters with specific threats leveled at Bank of America starting on September 18th, 2012 were available at http://pastebin.com/u/QassamCyberFighters); Tracy Kitten, *Alert: Banks at High Risk of Attack*, BANK INFO SECURITY (Sept. 20, 2012), http://www.bankinfosecurity.com/alert-banks-at-high-risk-attack-a-5128.

[54] *See* Strohm & Engleman, *supra* note 48, at 2.

[55] *Id.*

[56] PAUL K. KERR ET AL., CONG. RESEARCH SERV., R41524, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY 6 (2010).

was able to gain access to the computers controlling Iranian nuclear centrifuges before sending many of them spinning out of control, all while reprogramming the monitoring system to display and record normal operations.[57]

The complex operation targeted the ICS computers in two phases, both of which had to be executed with the additional hurdle of crossing an air gap, which meant that the computer data for both phases had to be physically installed into the machines via human beings (by spies or unwilling accomplices) wielding an infected laptop computer, thumb drive, or other data storage device that can feed the infected code into the control computers.[58] The first phase used a beacon program that created a meticulous electrical blueprint of the control computers and then "phone[d] home" the information so that it could be analyzed.[59] Once the information was received and analyzed and tests were successfully conducted on similar machinery, a second phase was executed whereby small variations were made in centrifuge speeds to cause numerous machines to eventually break down, with no two attacks looking exactly alike.[60]

Stuxnet allegedly set the Iranian nuclear program back two years,[61] illustrating the significance that this type of attack

---

[57] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.
[58] *Id.* (defining an air gap as a term for a system that is physically separated from the Internet).
[59] *Id.*
[60] *Id.*
[61] Yaakov Katz, *Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years*, THE JERUSALEM POST (Dec. 15, 2010, 5:15 PM),

can have to U.S. critical infrastructure. In particular, the Stuxnet's ability to infiltrate networks, identify specific ICSs, and launch attacks at opportune times can be replicated with catastrophic consequences for the ICSs that run U.S. critical infrastructure.[62] Such an attack in the future will be easier in one respect, since rather than being air-gapped, many U.S. critical infrastructure SCADA and other ICSs are connected to, and easily accessible, from the Internet, which includes the highly insecure Bluetooth wireless technology.[63] In addition, U.S. critical infrastructure does not routinely make use of security basics like data encryption.[64] For years, the U.S. critical infrastructure operators have been aware of these vulnerabilities in their ICS and SCADA systems but ignored them, because there was no evidence that other nations would exploit those flaws for sabotage.[65] Now, post-Stuxnet, regardless of whether or not the U.S. in fact spearheaded it, a peacetime cyber-arms race across the Internet could be kicking off, which can have serious implications for any vulnerable networks in the U.S.[66] The fact that the victim of Stuxnet, Iran,

---

http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475 (reporting that a consultant theorized the program would be set back by two years due to the need to scrub government and contractor computers of the virus as well as replace damaged equipment and centrifuges).

[62] *See* KERR ET AL., *supra* note 56, at 8.

[63] BRENNER, *supra* note 21, at 97.

[64] *Id.*

[65] BAKER ET AL., *supra* note 19, at 8, 10, 14.

[66] *See, e.g.*, Misha Glenny, *A Weapon We Can't Control*, N.Y. TIMES, June 24, 2012, *available at* http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html?_r=0 (arguing the U.S. "crossed a Rubicon" by firing the first shot in contemporary warfare with Stuxnet, tempting other countries that possess cyber-weapons to use them on vulnerable networks).

is now actively trying to attack U.S. interests through cyber-attacks on critical infrastructure comes as no surprise.[67]

Although no known cyber-attacks on U.S. critical infrastructure have come close to approaching the sophistication of Stuxnet, Iran has demonstrated the intent to resort to cyber-attacks on critical infrastructure and has shown that level of sophistication of Stuxnet is not a requirement to do so. One example is the DDoS attack on the U.S. banking system as discussed above.[68] Another example alleged to have been the work of Iran, and one that perhaps demonstrates an even clearer intent, is the August 2012 cyber-attack on the world's most valuable company, Saudi Aramaco, which erased all the data on three-quarters of the company's computers and replaced it with the image of a burning American flag.[69] The unsophisticated virus used in the attack, subsequently called "Shamoon," penetrated the Saudi Aramaco network through the Internet, targeted all the computers on its corporate network to wipe their hard drives at a specified time before reporting

---

[67] *See* Walter Pincus, *The Inevitable Blowback to High-Tech Warfare*, WASH. POST, Oct. 15, 2012, *available at* http://articles.washingtonpost.com/2012-10-15/world/35499943_1_stealth-drone-stuxnet-shamoon (correlating alleged U.S. cyber-attacks like Stuxnet with the alleged Iranian attacks against U.S. banks as well as the Shamoon attack on the Saudi Arabian oil company Aramaco).

[68] *See supra* text accompanying notes 45–50.

[69] Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES, Oct. 23, 2012, *available at* http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.

back through the first infected computer to the attackers of its success.[70]

The Shamoon attack alarmed government officials and computer experts because it had the potential to be far worse. Unlike the Telvent example described above,[71] Saudi Aramaco's oil production operations were fortunately segregated from the company's corporate network, so oil production was unharmed and no oil was lost.[72] Although the oil company attacked was a Saudi Arabian company, the burning American flag picture indicated the hackers' true target.[73] Richard Clarke, a former National Security Council counterterrorism official stated, "It proved you don't have to be sophisticated to do a lot of damage, [as] [t]here are lots of targets in the U.S. where they could do the same thing."[74]

Overall, the U.S. critical infrastructure has experienced enough significant attacks over the past several years to lend credibility to former Defense Secretary Panetta's warnings about the possibility of a "cyber–Pearl Harbor" event and render it more than mere hyperbole. The AURORA experiment proved the theory that U.S. critical infrastructure was vulnerable to cyber-attack. The string of attacks across several different sectors that have followed since, including banking, water resources and oil and gas pipelines, have demonstrated that those vulnerabilities are by no means limited to a single

---

[70] *See Shamoon Virus Targets Energy Sector Infrastructure*, BBC NEWS (August 17, 2012, 10:22 AM), http://www.bbc.co.uk/news/technology-19293797.
[71] *See supra* text accompanying notes 35–36.
[72] Perlroth, *supra* note 69.
[73] *See id.*
[74] *Id.*

sector. Both AURORA and Stuxnet demonstrated the sheer amount of damage that can be wrought through such an attack.

Additionally, both the AURORA experiment and some of the real-world cyber-attacks that followed demonstrated that no great technological sophistication is necessarily required; an Internet connection, a computer, and some general understanding of computer networks is often enough to wreak all kinds of disruption and/or damage. Actual cyber-attacks have also demonstrated that these vulnerabilities are clearly points of interest for a wide variety of different actors, including rival and enemy foreign governments, terrorist groups, and even lone hacktivists wanting to make a particular point. However, before one can discuss possible solutions, one must first undertake a discussion of what the key vulnerabilities are.

III. CYBER-VULNERABILITY FACTORS OF U.S. CRITICAL INFRASTRUCTURE

As already discussed, PDD-63 acknowledged that increasingly automated and linking of critical infrastructure systems to larger networks and the Internet resulted in its growing vulnerability to cyber-attack and directed that those vulnerabilities be eliminated.[75] This Part explores the key vulnerability factors that critical infrastructure systems face in the cyber dimension. Three vulnerability factors in particular stand out: (1) lack of robust cyber-threat information sharing; (2) Internet connectivity for ICS not designed with cybersecurity in mind; and (3) lack of critical infrastructure focus on cybersecurity.

---

[75] PDD-63, *supra* note 10, at 2.

A. Lack of Robust Cyber-Threat Information Sharing

Cyber-threat information sharing is the key to protecting critical infrastructure, because it yields a level of situational awareness that both the government and private sector need in order to effectively respond to light-speed cyber-attacks.[76] Once alerted to cyber-threats, government and private industry can rapidly collaborate through that same information sharing process to pool resources, analyze, and develop solutions for the afflicted party and those that might also be similarly vulnerable to such an attack.[77] Information sharing will also enable the government to be aware of the overall protection status of critical assets and how to best respond to cyber-attacks on critical infrastructure in the future.[78]

Information sharing in practice boils down to increased situational awareness about what computers are doing. The starting point would be to have both the government and private critical infrastructure monitoring their respective computer network traffic. The parties would, in real-time, scour their networks for both malicious computer code and unusual behavior, such as large volumes of e-mail traffic moving on the network in the middle of the night, that might be indicative of a DDoS attack. Information from these events would then be shared throughout government and critical

---

[76] BIPARTISAN POLICY CTR., CYBER SECURITY TASK FORCE: PUBLIC–PRIVATE INFORMATION SHARING 5 (2012), *available at* *http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf*.
[77] *Id.*
[78] *Id.*

infrastructure networks, including the malicious code captured and anything that can be discerned about it (e.g., what it does and what software vulnerabilities it might make use of), types of devices, operating systems being used, and the IP addresses or other information identifying the source of such activity. Information sharing can also include any identified patches or other "fixes" that may mitigate potential problem.

Collectively, the government and private industry can use the shared information "to look for trends, the prevalence of certain behaviors, and propagation patterns for malware."[79] For example, shared malicious code information can help power companies and water utilities to mitigate cyber-threats to their ICSs by identifying system vulnerabilities and the need for patches in similar software or systems across the entire industry. For suspicious behavior, the parties can assign threat scores to IP addresses or computers, similar to consumer credit ratings, and use the information "to block dangerous traffic and stop malicious activities."[80]

Since President Clinton signed PDD-63 in 1998, there has been an understanding early on that because so many critical infrastructure systems and facilities were outside of the government, elimination of those vulnerabilities would require close communication and coordination of efforts between the government and the private sector, and any partnership developed between private industry and government would

---

[79] Tim Molino, *Sharing Cyber Threat Information: How It Would Work, and Why It Would Help Bolster Security*, TECHPOST (Apr. 15, 2013), http://techpost.bsa.org/2013/04/15/sharing-cyber-threat-information-how-it-would-work-and-why-it-would-help-bolster-security.
[80] *Id.*

have to be "genuine, mutual and cooperative" to succeed.[81] The PDD-63 envisioned achieving this, to a great extent, through the creation of information sharing centers, where both the government and private sectors would gather, analyze, and disseminate threat and vulnerability information among each other.[82]

Specifically, the U.S. Government strongly encouraged the owners and operators of critical infrastructure to establish Information Sharing and Analysis Centers (ISACs) to act as a focal point for gathering and disseminating timely threat warnings and attack analysis of attacks for their respective sectors.[83] The Homeland Security Presidential Directive 7 (HSPD-7) in 2003 superseded to a large degree the government-sharing component established in PDD-63 and made the DHS responsible for all critical infrastructure coordination efforts.[84] The DHS in turn established the United States Computer Emergency Readiness Team (US-CERT) as the government focal point and charged it with collaboratively responding to cyber-incidents, providing technical assistance, and disseminating timely threat, exploit, and vulnerability information.[85] Ultimately, the hope was that the private sector information sharing centers would operate much like the Centers for Disease Control and Prevention (CDC), a technically-focused and trusted institution providing timely and

---

[81] PDD-63, *supra* note 10, at 3.
[82] *Id.* at 12–14.
[83] *Id.* at 13–14.
[84] *See* U.S. DEP'T OF HOMELAND SEC., HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 7: CRITICAL INFRASTRUCTURE IDENTIFICATION, PRIORITIZATION, AND PROTECTION (2003), *available at* http://www.dhs.gov/homeland-security-presidential-directive-7#1.
[85] *About Us*, US-CERT, http://www.us-cert.gov/about-us (last visited Aug. 22, 2014).

well-coordinated information and analysis aimed at strengthening the overall security and resiliency of all critical infrastructure from attack.[86]

Since 1998, distinct ISACs have been successfully created in most critical infrastructure sectors along the lines originally conceived.[87] However, although there is a lack of studies on the actual effectiveness of the ISACs in specific case studies, multiple reports have found that the system has not yet achieved the level of information sharing success that was originally envisioned.[88] In at least one very recent example, the massive DDoS attacks on the U.S. banking system discussed above,[89] the FS-ISAC only raised its alert level to its members on the day the attacks began, despite the fact that the attackers had broadcasted their intentions weeks before setting off the attacks and that some banks took heed of the threat and were better prepared for what ensued. At least one report further noted that the ISACs only share information internally with

---

[86] PDD-63, *supra* note 10, at 14.

[87] *See Member ISACs,* NATIONAL COUNCIL OF ISACS, http://www.isaccouncil.org/memberisacs.html (last Aug. 22, 2014) (listing current ISACs by sector along with a summary of their mission statements).

[88] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-827T, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES IN ADDRESSING CYBERSECURITY 14 (2005) (finding that effective communications between government and private critical industries are not yet in place in support of effective cybersecurity); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-383, INFORMATION SHARING: DHS SHOULD TAKE STEPS TO ENCOURAGE MORE WIDESPREAD USE OF ITS PROGRAM TO PROTECT AND SHARE CRITICAL INFRASTRUCTURE INFORMATION 17–20 (2006) (finding that various factors impede the private critical industry and government sharing components from sharing with the government effectively, including lack of trust, lack of understanding of what information should be shared, and private industry failure to see the benefits in sharing).

[89] *See supra* text accompanying notes 45–50.

members they specifically know and trust rather than distributing the information freely to all of their members simultaneously.[90] If that is true, it might help explain why some large banks were more prepared for the DDoS attacks than others.

A number of barriers to effective information sharing between the government and private industry persist that continue to make the stronger security apparatus originally envisioned elusive. Some of these barriers are a result of legal liabilities, of which some may only be speculative due to perceived legal ambiguities.[91] Additionally, the federal government itself is often viewed by the private industry as failing to live up to its responsibility to provide usable, timely, and actionable threat information for various reasons.

i. Legal Barriers to Information Sharing

Various sets of laws and legal liabilities currently exist, or are believed to exist, that deter and frustrate effective information sharing among private industry and between the private industry and the government. These potential liabilities arise from laws dealing with a diverse set of subjects, including antitrust laws, privacy laws, and private general negligence liability. Although many of these limitations may be less limiting than they are perceived to be, the result of these perceptions and, at the very least, the uncertainty about the state of the law as they pertain to information sharing, have

---

[90] BIPARTISAN POLICY CTR., *supra* note 76, at 10.

[91] PAUL ROSENZWEIG, KORET-TAUBE TASK FORCE ON NAT'L SEC. AND LAW, CYBERSECURITY AND PUBLIC GOODS: THE PUBLIC/PRIVATE "PARTNERSHIP" 14 (2011), *available at* http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf.

created collective inaction where individual companies often simply feel safer by keeping threat information to themselves rather than sharing it for mutual benefit.[92]

Private industry actors who want to collaborate to combat cybersecurity threats through information sharing often cite antitrust laws as an impediment.[93] The antitrust laws include the Sherman Act,[94] the Wilson Tariff Act,[95] and the Clayton Act,[96] which together generally forbid various types of agreements or other collusion among business competitors in a particular industry that result in the restraint of trade.[97] Section 5 of the Federal Trade Commission ("FTC") Act, prohibiting unfair and deceptive trade practices, is also frequently included, since courts have found that unfair competition includes activity in violation of the Sherman or Clayton Acts.[98] Industry actors fear something along the lines of the following general scenario regarding antitrust laws and information sharing:

> Company A voluntarily reports what may be a cybersecurity threat or incident in an information-sharing entity, such as in an ISAC. The ISAC membership includes competitors of

---

[92] BIPARTISAN POLICY CTR., *supra* note 76, at 5.
[93] EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 22 (2012), *available at* http://fas.org/sgp/crs/misc/R42409.pdf.
[94] 15 U.S.C. §§ 1–7 (2012).
[95] *Id.* §§ 8–11.
[96] *Id.* §§ 12–27.
[97] ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: DISCUSSION OF PROPOSED REVISIONS 23 (2012).
[98] *Id.*

> Company A. . . . A plaintiff claims that the information shared is an effort to harm competition and sues Company A for violating antitrust laws.[99]

A plaintiff in such a case might be a competitor, customer, or supplier in the same industry. The action may be taken up and investigated by either the FTC or the Federal Bureau of Information (FBI) or both, and can ultimately lead to an enforcement action by the FTC or civil and/or criminal actions filed by the Department of Justice.[100]

Some have also argued that privacy law, in particular the Electronic Communications Privacy Act's (ECPA) prohibitions on wiretapping[101] and access to stored communications,[102] are barriers to information sharing.[103] Generally, the wiretapping provisions prohibit communications providers such as Internet Service Providers (ISPs) from intercepting electronic communications in transit without proper legal authorization. Likewise, the stored communications provisions generally prohibit ISPs and other electronic communications services from disclosing electronic communications contents or subscriber information without legal authorization.

---

[99] INFO. TECH. INDUS. (ITI) COUNCIL, ITI RECOMMENDATION: ADDRESSING LIABILITY CONCERNS IMPEDING MORE EFFECTIVE CYBERSECURITY INFORMATION SHARING 3 (2012), *available at* http://www.itic.org/dotAsset/fae2feab-7b0e-45f4-9e74-64e4c9ece132.pdf.
[100] THOMAS V. VAKERICS, ANTITRUST BASICS § 2.01 (Law J. Press 1985).
[101] 18 U.S.C. §§ 2510–2522 (2012).
[102] *Id.* §§ 2701–2712.
[103] LIU ET AL., *supra* note 93, at 20.

In both cases, the law allows for lawful interception or disclosure of stored communications by ISPs in order to protect the rights and property of the provider of the service.[104] Additionally, while the wiretap provision, 18 U.S.C. § 2511(2)(a)(i), also allows for lawful interception and disclosure of communications when it is incident to providing service, the random monitoring of communications is limited to use only when performing service quality control checks.[105] Further, the stored communications provision, 18 U.S.C. § 2702(b)(7), allows disclosure of communication contents to law enforcement if the contents are "inadvertently obtained by the service provider" and "appear to pertain to the commission of a crime."[106] Another stored communication provision allows disclosure "to a government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure . . . ."[107] However, the potential for ambiguity in these provisions may hinder threat information sharing, particularly in the critical infrastructure realm.

One ambiguity that needs to be addressed is how broad the protection exception really is, particularly where the ISPs themselves are not the target of the cyber-threat in question.[108] An ISP might hesitate to voluntarily share cyber-threat information in a situation where a major bank appears to be targeted for a massive DDoS attack for fear that it might expose itself to the criminal penalties and private civil liability of violating the ECPA. An ISP might also hesitate to disclose

---

[104] 18 U.S.C. §§ 2511(2)(a)(i), 2702(b)(5).
[105] *Id.* § 2511(2)(a)(i).
[106] *Id.* § 2702(b)(7).
[107] *Id.* § 2702(b)(8).
[108] LIU ET AL., *supra* note 93, at 22.

the malware detected in an email to a utility while they try to discern whether the malware constitutes commission of some crime or whether a good-faith belief of danger to life might exist. Thus, the current exceptions to the ECPA do not lend themselves particularly well to the protection of critical infrastructure beyond the communications sector.

Lastly, private industry actors often cite their fear of simple negligence-based lawsuits as a barrier to effective information sharing.[109] The "foreseeability of consequences" is generally an essential factor in defining the existence and extent of liability in a given negligence case.[110] A duty generally arises for defendants to act reasonably in the face of a foreseeable risk.[111] Conversely, the absence of any foreseeable risk means that the defendant often has no duty to mitigate that risk.[112] However, if a defendant is found to have had knowledge of a risk and its preventative measures ahead of time, a higher standard of care generally applies than if the defendant had no such information.[113]

Applied to the information sharing and critical infrastructure realm, where a power plant owner receives notice and information about a particular vulnerability in his

---

[109] *See* Eric Engleman, *Companies Want Lawsuit Shield to Share Cyber Threat Data*, BLOOMBERG BUS. WK. (Mar. 7, 2013), http://www.businessweek.com/news/2013-03-07/companies-want-lawsuit-shield-to-share-cyber-threat-data.

[110] D.E. Buckner, Annotation, *Foreseeability as an Element of Negligence and Proximate Cause*, 100 A.L.R.2d 942 § 1 (2013).

[111] *Id.*

[112] *Id.*

[113] LIU ET AL., *supra* note 93, at 24. S*ee, e.g.*, Rodriguez v. New Haven, 439 A.2d 421, 424 (Conn. 1981) ("Knowledge of a dangerous condition generally requires greater care to meet the standard of reasonable care.").

operating system, this would tend to show that the risk from a cyber-attack using that vulnerability was foreseeable and might create a duty for the power plant owner to patch or otherwise mitigate the vulnerability. If the vulnerability is subsequently exploited and a power surge from the plant, for example, ended up severely injuring people, the owner of the facility may be liable for negligence based on his knowledge. As a result, the power plant has an incentive to not meaningfully participate in information sharing by simply staying in the dark and not expose itself to potential liability.

That same liability, however, may also operate in reverse for the actor that actively shares the vulnerabilities that it discovers in its own systems and reports them to an ISAC or government agency. Reporting vulnerabilities may create a heightened duty for the power plant to mitigate that risk somehow and may have its own disclosure potentially used against it in court. As a result, two or more power plants may have the same control system vulnerability, but the ones that do not share might very well be viewed as cyber-secure by default from a negligence liability standpoint while the reporting plant may potentially face greater liability.

The ISACs themselves may even be subject to liability. Some ISACs have begun acting as clearinghouses by collecting and distributing information, such as IP addresses and domain names that distribute malware or are sources of other cyberthreats, to their sector members.[114] However, similar successful nonprofit based efforts in this area, such as the Anti-Phishing Working Group, have been threatened with lawsuits by domain name owners and companies who have been

[114] BIPARTISAN POLICY CTR., *supra* note 76, at 9.

identified as threat sources but also host innocuous websites.[115] Due to the perceived potential for lawsuits, the ISACs who are aggregating such information only share their information with members they trust rather than sharing more broadly across the whole sector or with government entities.[116] Overall, because of the perceived and actual legal risks, the safer bet for many in private critical infrastructure is to minimally participate in information sharing activities.

ii. Governmental Barriers to Information Sharing

There are also some key barriers that prevent effective cyber-threat information sharing from the government to the critical infrastructure owned by the private sector. In regards to cyber-threats and information sharing, a 2010 U.S. Government Accountability Office (GAO) report found that the private industry critical infrastructure operators expect the government to provide "usable, timely, and actionable cyber-threat information and alerts . . . and a single centralized government cybersecurity organization to coordinate federal efforts."[117] However, only 27 percent of the industry reported that they were receiving actionable cyber-threat information or

---

[115] *Id.*
[116] *Id.* at 10.
[117] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-628, CRITICAL INFRASTRUCTURE PROTECTION: KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS NEED TO BE CONSISTENTLY ADDRESSED 14 (2010) [hereinafter GAO KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS] (conducting structured interviews and surveying fifty-six private sector representatives from the following critical infrastructure sectors: (1) banking and finance, (2) communications, (3) defense industrial base, (4) energy, and (5) information technology, all of which were members of the ISACs and sector councils).

alerts to at least a moderate extent.[118] Perhaps most alarming of all, the private industry reported confusion regarding where to even receive government cyber-threat information due to so many different agencies working independently in this area.[119]

The first problem is that the critical infrastructure does not receive useful or actionable cyber-threat information or alerts. According to the National Infrastructure Protection Plan (NIPP), the stated goal of the government is to provide exactly the kind of information the private sector is looking for.[120] However, what the private critical infrastructure is actually receiving is not detailed or timely enough to each individual sector to allow comprehension of what tactics and techniques are being used or even what actions can be taken to protect their networks.[121]

There are a number or reasons for this current state of affairs. DHS officials have stated that the US-CERT is "impacted by restrictions that do not allow individualized treatment of one private sector entity over another private sector entity—making it difficult to formally share specific information with entities that are being directly impacted by a cyber-threat."[122] Additionally, the US-CERT's extensive coordination and review process results in untimely reporting, "potentially adding days to the release if classified or law

---

[118] *Id.* at 16.
[119] *See id.* at 15.
[120] NATIONAL INFRASTRUCTURE PROTECTION PLAN, *supra* note 5, at 10 (stating that the government aims to assist the critical infrastructure by "[p]roviding owners and operators with timely, accurate, and useful analysis and information on threats").
[121] GAO KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS, *supra* note 117, at 16.
[122] *Id.* at 17.

enforcement information must be removed from the product."[123]

Further, the classification of information itself is a serious problem and a significant contributor to the current untimeliness of the warnings. While large majorities of private defense contractor personnel have clearance to access classified information, few in the electricity generation and transmission companies do, much less other critical infrastructure sectors.[124] Agencies, such as the FBI, the DoD, or the Central Intelligence Agency (CIA), that own classified or law enforcement information germane to a particular warning must be coordinated with as part of the review process, which can add days to the release time of the information.[125] For example, one consumer of the US-CERT warnings stated that the alerts "generally arrive a day or two after they might have been helpful."[126] Another consumer stated that, in some cases, they resort to the media for cyber-incident information because the media often puts out such information more quickly than the US-CERT does.[127]

The sanitation of these reports of classified and law enforcement information have not only the potential to make the alerts untimely but they may often also rob the reports of

---

[123] *Id.* at 17–18.
[124] BIPARTISAN POLICY CTR., *supra* note 76, at 13.
[125] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-588, CYBER ANALYSIS AND WARNING: DHS FACES CHALLENGES IN ESTABLISHING A COMPREHENSIVE NATIONAL CAPABILITY 41 (2008) [hereinafter GAO CYBER ANALYSIS AND WARNING].
[126] *Id.*
[127] *Id.*

any information actually useful to industry.[128] For example, concern that a warning release may alert intruders to their discovery and the existence of an ongoing investigation might prompt a law enforcement agency, such as the FBI, to withhold certain technical details that might be crucial to defending networks.[129] An investigation may even preclude any warning release at all. Although the 2011 South Houston water treatment plant hack was reported in the press, which was investigated by both the FBI and the Industrial Control System Cyber Emergency Response Team (ICS-CERT) and dissected at a government ICS conference the following spring, no report or warning was apparently ever issued regarding the event.[130] In contrast, in a similar investigation into a pump failure at an Illinois water treatment plant, ICS-CERT did release a report emphatically stating there was no evidence of any cyber-intrusion.[131] Thus, the lack of any report or warning despite an investigation in the South Houston case is puzzling.

A significant part of the US-CERT's mission is to "coordinate and collaborate" with critical infrastructure owners and operators, but this is rarely accomplished because the US-CERT is buried within the DHS and has no authority to compel sector-specific federal agencies or law enforcement to coordinate and cooperate with the US-CERT's activities.[132] As

---

[128] GAO KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS, *supra* note 117, at 17.
[129] GAO CYBER ANALYSIS AND WARNING, *supra* note 125, at 41.
[130] *See supra* text accompanying notes 41, 44.
[131] *See* U.S. DEP'T OF HOMELAND SEC., ICSB-11-327-01: ILLINOIS WATER PUMP FAILURE REPORT (2011), *available at* http://ics-cert.us-cert.gov/tips/ICSB-11-327-01.
[132] *Examining the Cyber Threat to Critical Infrastructure and the American Economy: Hearing before the H. Comm. of Homeland Security, Subcomm. on Cybersecurity, Infrastructure Protection, and Security Technologies*,

a result, the US-CERT's efforts to promulgate warnings are limited by other federal entities' ability and authority to determine specific cyber-threats to the critical infrastructure under their oversight, but there are no verified and widely accepted practices for performing cyber-threat analysis.[133] Additionally, these agencies sometimes lack sufficiently cleared personnel to coordinate classified materials that might be relevant to the sector. But even if not, such personnel are usually in the highest echelons of the organization as opposed to those with a cybersecurity or information security background who can adequately comprehend the information or handle the mitigation efforts.[134]

Additionally, while DHS leadership previously proposed broadening the role and focus of the US-CERT by having it provide centralized monitoring role for the entire federal government, subsequent DHS leadership ultimately decided that each federal agency should have its own 24-hour-a-day, 7-day-a-week incident-handling capability (either in-house or contracted out) to respond to incidents affecting its own network.[135] As such, certain agencies such as the State Department, Justice Department, and Federal Aviation Administration have developed a much higher technical monitoring and response capability than the US-CERT.[136] This duplication of effort and capability diminishes the US-CERT's ability to act as central focal point for government

---

112th Cong. 50 (2011) [hereinafter *Testimony of Mischel Kwon*], *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf (testimony of Mischel Kwon, President, Mischel Kwon & Associates, LLC).

[133] GAO CYBER ANALYSIS AND WARNING, *supra* note 125, at 42.

[134] *Id.* at 41–42.

[135] *Id.* at 46.

[136] *Testimony of Mischel Kwon*, *supra* note 132, at 49.

cybersecurity-related critical infrastructure protection efforts and deprives it of valuable resources such as funding, technical capability, and access to the best personnel.[137]

Perhaps most troubling of all is the apparent industry confusion from where to even receive government cyber-threat information despite the fact that the US-CERT is supposed to be the government focal point for that function. There are too many government agencies with different cyber-missions working independently, with project duplication to the point that it is not uncommon for several different groups to be working on the same thing, unaware of each other's efforts.[138] A recent DHS Inspector General (IG) report regarding ICSs found that the owners and operators of critical infrastructure may have to look across a host of different agency and sector-sharing portals to retrieve and compile applicable advisories, vulnerability information, and best practices.[139]

The following example provides additional insight into the extent of this problem. The Homeland Information Security Network (HSIN) is a secure portal for cyber-threat information sharing and collaboration and is distinct from the US-CERT and a multitude of other DHS and federal agency information

---

[137] GAO CYBER ANALYSIS AND WARNING, *supra* note 125, at 46; *Testimony of Mischel Kwon*, *supra* note 132, at 49–50 (testifying that cybersecurity components at the DHS are too bogged down in other DHS mission spaces and suffer from a quagmire of internal politics and jostling for resources and mindshare).

[138] GAO KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS, *supra* note 117, at 17.

[139] U.S. DEP'T OF HOMELAND SEC., OIG-13-39, DHS CAN MAKE IMPROVEMENTS TO SECURE INDUSTRIAL CONTROL SYSTEMS 6–7 (2013) [hereinafter OIG DHS CAN MAKE IMPROVEMENTS], *available at* http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-39_Feb13.pdf.

sharing mechanisms that currently exist but do not coordinate their efforts.[140] Under a subset of the HSIN, the HSIN–Critical Infrastructure, there are currently fifty-five distinct information sharing communities that must be individually searched for pertinent and updated cyber-threat information, which is often found in portals among other non-cyber-security information and products.[141] An operator of a natural gas power plant might naturally be interested in cyber-security information from multiple sectors and subsectors such as the Oil and Natural Gas, Emergency Management, and Electricity. Individually searching all of the potentially applicable portals for pertinent cyber-security information, not to mention those of other agencies that might also contain applicable information, is cumbersome and time-consuming.[142]

The current model of information sharing is falling short of the efficient, well-coordinated, and effective process originally conceived. From the standpoint of private critical infrastructure, although they agree that information sharing is important, the benefits of sharing are often difficult to discern while the risks and costs of sharing are more direct and foreseeable.[143]

---

[140] *See generally Homeland Security Information Network*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/homeland-security-information-network (last visited Aug. 25, 2014).
[141] OIG DHS CAN MAKE IMPROVEMENTS, *supra* note 139, at 7.
[142] *Id.* at 6–7.
[143] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-780, CRITICAL INFRASTRUCTURE PROTECTION: IMPROVING INFORMATION SHARING WITH INFRASTRUCTURE SECTORS 10 (2004); ISAC COUNCIL, VETTING AND TRUST FOR COMMUNICATION BETWEEN ISACS AND GOVERNMENT ENTITIES 2 (2004), *available at* http://www.isaccouncil.org/images/Vetting_and_Trust_013104.pdf.

B. Cyber-Insecure Industrial Control Systems

The current state of cyber-security for ICSs is another key factor that needs to be addressed. ICSs, like SCADA, are of crucial importance because they automate, manage, and perform vital operations across many of our nation's critical infrastructure. Currently, only personnel such as a night watchman physically inspects the operation of controllers occasionally, whereas the continuous process of checking and controlling is done solely by ICSs communicating with other machines and computers.[144] In oil and natural gas distribution, ICSs might perform a function as straight forward as monitoring and controlling pressure and flow through pipelines or they can be more complicated and expansive. In electricity generation, SCADA systems exercise supervisory control over a multitude of diverse and dispersed components in different locations, managing and controlling nearly all aspects of "generation, transmission, and distribution of electric power . . . by opening and closing circuit breakers and setting thresholds for preventive shutdowns."[145] As a result, the ICSs in electricity infrastructure must perform all of these functions at an expected 99.9999 percent reliability rate.[146] As Stuxnet demonstrated, slight unintended modifications to the operation of ICSs can have disastrous consequences for the machines that they run.

---

[144] BRENNER, *supra* note 21, at 96.
[145] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-628T, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES AND EFFORTS TO SECURE CONTROL SYSTEMS 8 (2004) [hereinafter GAO CHALLENGES TO SECURE CONTROL SYSTEMS].
[146] JOSEPH WEISS, PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS 8 (Momentum Press 2010).

In 2007, although the AURORA experiment showed that risks traditionally identified in the information technology realm were also becoming risks to operational technology, ICSs remain unreasonably vulnerable to cyber-attack.[147] Even when the critical industry is adequately informed about a particular vulnerability in their ICS, addressing the problems takes far too long. A study by Red Tiger Security, a company that audits critical infrastructure cyber-security, found that the patch time for oil and electric utilities was 331 days on average, with one oil refinery taking seven years to patch a single known vulnerability.[148] One factor for this state of affairs is the increasing interconnectivity of ICSs through the Internet for systems that were not designed with cybersecurity in mind. A second factor is the private industry's failure to adequately address the issue or even admit that such an issue even exists.[149]

i. Internet Connectivity for Cyber-Insecure Systems

Starting around the turn of this century, ICSs began being interconnected to the Internet and other networked computing systems were implemented as a means of lowering costs and improving efficiency by putting operations-related

---

[147] BRENNER, *supra* note 21, at 94–95.

[148] Andy Greenburg, *Electric, Oil Companies Take Almost a Year to Fix Hackable Security Flaws*, FORBES (July 28, 2010, 1:43 PM), http://www.forbes.com/sites/firewall/2010/07/28/electric-oil-companies-take-almost-a-year-to-fix-known-security-flaws.

[149] RALPH LANGNER & PERRY PEDERSON, CTR. FOR 21ST CENTURY SEC. AND INTELLIGENCE, BOUND TO FAIL: WHY CYBER SECURITY RISK CANNOT SIMPLY BE "MANAGED" AWAY 2 (2013), *available at* http://www.brookings.edu/~/media/research/files/papers/2013/02/cyber security langner pederson/cybersecurity_langner_pederson_0225.pdf.

information at the management's fingertips for better systems auditing and cost management.[150] Increased connectivity also allowed engineers and other staff to monitor and control systems from different points on the network, meaning greater coverage and more rapid diagnostics, maintenance and system status support for numerous remote and local facilities simultaneously.[151] Further, through the Internet or wide area networks and hand-held devices, the data sharing and support can occur from virtually anywhere.[152] In the electricity generation realm, the interconnectivity has also been particularly beneficial for customers by helping to break the local monopolies of the past; users now have access to the same transmission information that the utilities have, allowing customers to purchase electrical power from whomever.[153]

---

[150] *Cybersecurity: Assessing our Vulnerabilities and Developing an Effective Response: Hearing before the S. Comm. on Commerce, Science, and Transportation*, 108th Cong. 12 (2009) [hereinafter *Weiss Statement to S. Comm. on Cybersecurity*], *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg50638/html/CHRG-111shrg50638.htm (statement of Joseph M. Weiss, control systems cybersecurity expert).

[151] GAO CHALLENGES TO SECURE CONTROL SYSTEMS, *supra* note 145, at 13.

[152] *Id.*

[153] *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-926T, CYBERSECURITY: CHALLENGES IN SECURING THE ELECTRICITY GRID 4–5 (2012) [hereinafter GAO CHALLENGES IN SECURING THE ELECTRICITY GRID] (stating that the "smart grid" is an ongoing initiative that uses IT networks to provide system operators with more detailed data on the conditions of the transmission and distribution systems and better tools to observe the overall condition of the grid, and automated switches that communicate with each other to reroute electricity rapidly, which includes benefits such as fewer and shorter outages, lower electricity rates for customers resulting from the ability to shift peak demand, and an improved ability to shift to alternative sources of energy).

Unfortunately, this change in critical infrastructure ICS environment has resulted in an increase in the available avenues for cyber-attack. Organizations who have open access links for remote diagnostics and maintenance of ICS can be exploited by hackers to either take direct control of the systems, as occurred in the suburban Houston water treatment plant example, or provide an easy doorway for malicious code insertion, as in the case of Stuxnet. The change in environment has also resulted in an increase in the number of vulnerabilities available for hackers to exploit. ICSs are particularly vulnerable to such attacks because they often lack the capability to implement modern basic cyber-security technologies such as authentication,[154] encryption,[155] or in some cases, up-to-date operating systems or even the ability to patch or upgrade them.[156]

ICSs lack these technologies because of the key differences between the way ICSs and more traditional information technologies were developed and used. ICSs that monitor and control critical infrastructure processes were traditionally operated in a stand-alone environment, where computer systems communicated exclusively with other computer systems connected to the control system network..[157] Since ICSs have traditionally been intensely focused on simplicity, efficiency, and reliability above all else, and

---

[154] Computer security authentication means verifying the identity of a user logging onto a network and examples of this include passwords, digital certificates, smart cards and biometrics.

[155] Encryption is a way to protect information by encoding it; to anyone but the recipient with the correct key, the information looks like a random series of letters, numbers and characters.

[156] *Weiss Statement to S. Comm. on Cybersecurity*, *supra* note 150.

[157] US-CERT, CONTROL SYSTEMS CYBER SECURITY AWARENESS 3 (2005), *available at* http://www.controlglobal.com/whitepapers/2006/039.html.

because of the isolation of the systems, security was focused on physical access as opposed to cybersecurity.[158]

Specifically, physical security was viewed as more important because ICSs were historically comprised of proprietary hardware and software developed for specific companies by vendors, and knowledge of these proprietary applications was limited to a small population and not readily available to the general population.[159] Because the systems were physically isolated and required significant effort to discover the vulnerabilities in these proprietary systems before very specific tools could be developed to exploit them, cyber-attacks were viewed as unlikely and little attention was focused on cybersecurity.[160]

More recently, in an effort to reduce costs, companies that use ICSs have been switching from proprietary systems to standardized technologies such as Microsoft Windows and common Internet networking protocols. These widely available standardized technologies have commonly known vulnerabilities and exploitation tools for these vulnerabilities readily available for use.[161] Thus, not only has the number of people knowledgeable enough to wage cyber-attacks on critical infrastructure that use ICS increased significantly but the use of standardized technology also eliminates the need to specifically prepare for a particular target.[162]

---

[158] *Id.*
[159] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-354, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES AND EFFORTS TO SECURE CONTROL SYSTEMS 12 (2004).
[160] *See id.*
[161] *Id.*
[162] *Id.*

Unlike the rapid advancement and turnover in typical computers, ICS devices may be twenty years old or more before replacement, and because of their age and simplicity, they were not designed with sufficient processing power and memory for modern security applications.[163] Operating systems are also problematic in ICSs. Many ICSs are utilizing unpatchable and unsecurable operating systems such as Windows 95 and 97, which were designed and built into larger system packages and cannot be replaced, much less updated, without replacing the entire system.[164] Even for systems that can be patched or have a physical port through which to install patches, many patches would do more harm than good, as the operating systems have usually already been significantly modified by the ICS vendors.[165] Further, patches installed in violation of vendor support agreements (i.e., not developed directly by the vendor) often result in voiding the agreements for any consequences that may result.[166]

Adding security applications, such as anti-virus software, also presents problems, even for systems that have the ability to do so. Currently, but for a small subset of components, most ICS vendors do not offer anti-virus support.[167] For many systems, adding anti-virus software after the fact without vendor support can result in malfunction of the

---

[163] *Weiss Statement to S. Comm. on Cybersecurity*, *supra* note 150.
[164] *Id. See generally* ANDREW GINTER, CHIEF SEC. OFFICER, INDUS. DEFENDER, AN IT PERSPECTIVE OF CONTROL SYSTEMS SECURITY 3 (2009), *available at* http://www.controlglobal.com/whitepapers/2010/015.
[165] *Weiss Statement to S. Comm. on Cybersecurity*, *supra* note 150 (citing specifically an example of a water treatment plant that installed a patch only to discover that they were able to start but not stop the pumps).
[166] GAO CHALLENGES TO SECURE CONTROL SYSTEMS, *supra* note 145, at 19.
[167] GINTER, *supra* note 164, at 3.

ICS due to compatibility problems.[168] Even basic authentication practices, such as changing default vendor passwords for the ICS, are not implemented, because every engineer, technician, or operator needs to have the ability to rapidly access a critical component in an emergency to potentially avert a catastrophe.[169]

Thus, patching and securing ICSs is not as simple as it often is for personal home computers or even large office networks, which often can be done automatically or upon being accepted by users with the simple click of mouse and with little downtime or user inconvenience. On the other hand, ICSs in critical infrastructure have to run with a very high rate of reliability not expected of other computers. Further, because of ICSs' incorporation into large and complex machine systems with no downtime, they cannot afford to go offline to test patches that can cause serious problems when implemented in real-time.[170]

Overcoming the cyber-insecurity prevalent in ICSs requires intimate familiarity with the particular ICS and the processes that they automate; it is not a matter of simply repackaging and thrusting existing information technologies

---

[168] *Id.*
[169] *Id.* at 4.
[170] Greenburg, *supra* note 148; GINTER, *supra* note 164, at 3 (stating that patches for ICS, if they can be applied, are applied slowly and deliberately to ensure the safe continued operation of the system involved). For example, if available, a test bed system is "first be patched and tested" before "a patch may be applied on one system in a redundant set," and that system would be watched closely for a period of time. *Id.* If the system is able to "behave within specification across a wide range of operational conditions," the patch may then be applied to other systems in the redundant set over a period of several months. *Id.*

and practices into ICSs to make them secure.[171] Research and development will be necessary to bridge the gap that exists between currently available security technologies and what will be necessary to ultimately secure ICSs.[172] Any such development will have to fragment its focus on what security technologies are needed across various ICS applications, with experts in particular ICSs "determining acceptable performance trade-offs" for added security and "recognizing attack patterns for use in intrusion detection systems."[173]

Additionally, there will be a lengthy and costly process of migrating to the newer systems required to make ICSs secure, which does not fit well with the bottom-line and competitive pricing driven business plans prevalent in the electricity and other critical infrastructure sectors.[174] Not only will new components have to be developed and purchased, but many ICSs will also have to be replaced prematurely and more personnel will have to be hired to make and maintain the transition.[175]

Finally, for ICS cybersecurity to improve, both the vendor engineers who design the ICSs and the facility engineers who maintain ICSs need to have a significantly greater grasp of cybersecurity, which traditionally has only been a concern for Information Technology (IT) professionals.[176] Therefore, more training programs have to be developed to fill the current lack of ICS cybersecurity college

---

[171] *Weiss Statement to S. Comm. on Cybersecurity*, *supra* note 150.
[172] GAO CHALLENGES TO SECURE CONTROL SYSTEMS, *supra* note 145, at 19.
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Weiss Statement to S. Comm. on Cybersecurity*, *supra* note 150.

curricula or ICS cyber-security professional certification programs.[177]

ii. Failure to Address ICS Cybersecurity

While connectivity for ICS has created tremendous efficiencies from the standpoint of customers and business, the process is being pursued without the question of "why an executive in the Boardroom would want to control a valve in a plant or open a breaker in a substation" being meaningfully addressed.[178] In other words, little has been done in practice to regulate or mitigate the cybersecurity risk that the added efficiency creates.

The regulatory scheme regarding ICS cybersecurity is often slow and cumbersome. The North American Electric Reliability Corporation (NERC) is composed of the owners and operators of the electricity grid and is charged with developing and enforcing mandatory cybersecurity standards collaboratively through a process involving utilities and others in the electricity industry.[179] The NERC, in turn, is subject to

---

[177] *See id.*; *see also* BOB LOCKHART & BOB GOHN, PIKE RESEARCH CLEANTECH MARKET RESEARCH, MONITORING AND SECURING SCADA NETWORKS 15 (2011), *available at* http://www.ndm.net/siem/pdf/wp-pike-monitor-secure-scada-networks.pdf (claiming that examples of current certifications offered in this area include Certified Information Systems Auditor (CISA) offered by the Information Systems Audit and Control Association (ISACA) and Global Information Assurance Certification (GIAC) from ISACA as well, which generally require several years of control system experience and passing a challenging exam).

[178] *Weiss Statement to S. Comm. on Cybersecurity*, *supra* note 150.

[179] *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-117, ELECTRICITY GRID MODERNIZATION: PROGRESS BEING MADE ON CYBERSECURITY GUIDELINES, BUT KEY CHALLENGES REMAIN TO BE

oversight by the Federal Energy Regulatory Commission (FERC), which either approves cybersecurity standards developed by the NERC or directs them to modify it.[180] The FERC has also works in concert with the NIST to independently develop cybersecurity standards, but those standards must then be re-adopted by the NERC before they can become enforceable.[181] Thus, cybersecurity standards ultimately only become mandatory and enforceable after they are developed by the NERC and then approved by the FERC.

Although the FERC approved a basic set of cybersecurity standards developed by the NERC in 2008, there has since been little subsequent progress; the FERC has directed the NERC to make numerous changes to cybersecurity standards that still had not been implemented four years after they had been approved.[182] The NERC itself defers to an industry membership that has no desire to have its ability to connect ICSs to the Internet restricted, therefore the NERC has not developed any such restrictions.[183] Pure governmental initiatives aside from the NERC have not fared much better. A GAO report in 2011 found that a cybersecurity standards initiative developed over a two-year period by the NIST and considered by the FERC for adoption was running behind schedule and failed to address several key elements.[184]

ADDRESSED 11 (2011) [hereinafter GAO ELECTRICITY GRID MODERNIZATION].

[180] *Id.*

[181] *Id.* at 18–19.

[182] GAO CHALLENGES IN SECURING THE ELECTRICITY GRID, *supra* note 153, at 13.

[183] BRENNER, *supra* note 21, at 100.

[184] GAO ELECTRICITY GRID MODERNIZATION, *supra* note 179, at 15–16 (holding that specifically, the standards failed to address the risk of

This cumbersome and slow-moving process of developing cybersecurity standards has raised concerns as to whether the standards can adequately address the rapidly evolving threats.[185] There are also concerns that the process focuses on utilities with minimum regulatory compliance instead of designing a comprehensive and effective cybersecurity approach that actually works for each utilities' unique systems.[186] Consequently, a regulatory-mandated minimum-security approach creates requirements that are inherently incomplete, which, in addition to "having a culture that views the security problem as being solved once those requirements are met will leave an organization dangerously vulnerable to cyber-attack."[187]

Outside of the energy sector, the regulatory schemes for cybersecurity are less clear. While some critical infrastructure sectors that use ICSs, such as dams, fall under the same scheme as energy, other sectors have little, if any, meaningful federal oversight schemes at all.[188] For example, a 2008 GAO report found that the drinking water and water treatment sector was only regulated in terms of cybersecurity by a single 2002 law requiring water systems to self-assess vulnerabilities, which

---

combined cyber-physical attacks, as well as research and development and supply-chain vulnerabilities, because it would have caused the agency to be even further behind schedule.).

[185] *Id.* at 23.

[186] *Id.*

[187] *Id.* at 23–24.

[188] *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-1075R, INFORMATION TECHNOLOGY: FEDERAL LAWS, REGULATIONS, & MANDATORY STANDARDS FOR SECURING PRIVATE SECTOR INFORMATION TECHNOLOGY SYSTEMS & DATA IN CRITICAL INFRASTRUCTURE SECTORS (2008).

included risks to their ICSs.[189] Beyond that, it would presumably fall to individual local or state governments to set and enforce any cybersecurity standards for ICS in their water systems.

IV. ADDRESSING THE VULNERABILITY FACTORS

"The new Congress must take up this issue, and pass comprehensive [cybersecurity] legislation to defend our nation against this gathering cyberthreat. If it doesn't, the day on which those cyberweapons strike will be another "date which will live in infamy," because we knew it was coming and didn't come together to stop it."

- Senators Joseph I. Lieberman and Susan Collins[190]

Ineffective information sharing and cyber-insecure ICS are areas of incredible vulnerability in critical infrastructure in desperate need of addressing. As demonstrated in Part II, current information sharing between private industry and government actors is too wrought with obstacles to rise to the level of situational awareness necessary to respond in an era of fast-moving and ever accelerating cyber-attacks. Additionally, the ICSs that run and maintain many critical infrastructure processes have been proven unprepared for the era of added Internet connectivity in the name of efficiency. Efforts to address the cyber-insecurity of ICSs have fallen far short of providing any effective cybersecurity for those systems. These

---

[189] *Id.* at 24 (showing that the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 required community water systems serving more than 3300 people assess its vulnerability to an intentional act meant to substantially disrupt its safe supply of drinking water, which included a review of any electronic, computer, or other automated systems utilized).

[190] Lieberman & Collins, *supra* note 18.

problems are magnified by the fact that terrorists, opposing nation states, and even hacktivists are actively exploring and exploiting these vulnerabilities in pursuit of their agendas.

This Article proposes that legislation is necessary to overcome these vulnerabilities. Specifically, legislation that implements two factors: (1) centralized and mandatory threat communication that is carefully tailored, and (2) government-incentivized, but private industry-developed, security.

A. Why the Executive Order is an Insufficient Answer

PDD-63 and similar policies published by successive Presidents have recognized the need to address critical infrastructure cybersecurity and either put in place or adjust frameworks or both in order to do so.[191] On February 12, 2013, President Obama upped the ante over previous efforts with an Executive Order ("Order") specifically titled "Improving Critical Infrastructure Cybersecurity."[192] The Order is specifically designed to strengthen the critical infrastructure cyber-defenses through increased information sharing and cybersecurity standards development.[193] With issuance of the Order, is legislation is really necessary?

---

[191] *See supra* text accompanying notes 10–13.

[192] Exec. Order No. 13,636, 78 C.F.R. 11,737 (2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[193] Obama, *supra* note 14. *See generally* ERIC A. FISCHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 8–10 (2013) (specifying that the implementation of the Executive Order No. 13,636 will be consistent with the applicable law and that nothing in the Order provides regulatory authority to an agency beyond that under existing law).

The Order purports to improve and increase information sharing in several ways. First, the DHS, the Attorney General, and the Director of National Intelligence (DNI) are ordered to streamline the process of disseminating timely and useful unclassified threat reports to private sector owners and operators of critical infrastructure.[194] To maximize the utility of the information provided in those reports, the Order also expands the use of sector subject matter experts to advise on the types of information most useful to owners and operators in those sectors.[195] Finally, the Order expands the Enhanced Cybersecurity Services (ECS) program, a comprehensive information sharing program previously confined to the Defense Industrial Base (DIB), to use in all critical infrastructure sectors.[196]

If the process of providing unclassified reports is quicker, and the reports incorporate tailored input from sector subject matter experts to make them more useful to the respective industry, the Order would, to a certain extent, overcome the governmental burdens to information sharing that currently exist and satisfy the private sector's desire for more timely and quality information it can use. Likewise, increased availability of security clearances and participation in ECS by critical infrastructure actors would also likely contribute positively to the quality and timeliness of cyber-threat information.

---

[194] Exec. Order No. 13,636, *supra* note 192, at § 4(b).
[195] *Id.* § 4(e).
[196] *Id.* § 4(c). *See* FISCHER ET AL., *supra* note 193, at 6 (explaining that under the DIB program, the DOD/NSA "provides defense contractors with classified and unclassified cyber-threat information and cybersecurity best practices," and in turn, the DIB participants "report cyber-incidents, coordinate on mitigation strategies, and participate in cyber intrusion damage assessments if DOD information is compromised").

Unfortunately, a number of government barriers remain unaddressed. While the Order is intended to make a subset of information sharing more robust, it may fall far short of what is necessary to make information sharing truly effective across the board. For those in critical infrastructure who do not qualify for the ECS program or those that simply choose not to apply, there is also the problem of insufficient integration between a great number of existing information sharing portals and bodies. Thus, the Order seems to create yet another information sharing body without attempting to sort out, streamline or otherwise reform the cumbersome and confusing information sharing structure already in place.

In reality, the Order barely affects the legal barriers to information sharing by the private industry, which may be beyond the unilateral reach by executive action in the first place.[197] The Order creates no safe harbors, liability limitations, or exclusions, thereby likely failing to assuage any of the private industry's likely concerns about participation in information sharing. In fact, the Order may increase hesitation on the part of the private industry due to the publication of the recommendations or risk assessments called for in the Order, as litigants can use those as evidence of appropriate care standards in general tort litigation against members of the private industry even if the standards are not ultimately controlling.[198]

---

[197] FISCHER ET AL., *supra* note 193, at 9.

[198] *Id. See, e.g.*, Burmaster v. Gravity Drainage Dist. No. 2, 448 So. 2d 162, 164 (La. Ct. App. 1984) (holding that the Occupational Safety and Health Act regulations and standards published by industry groups warrant consideration as evidence of standard of care, even if they are not controlling).

The Order also envisaged stronger cybersecurity standards by having the NIST lead the development of a cybersecurity framework ("Framework") and gave the NIST 240 days to craft the standards, which were subsequently published on February 12, 2014.[199] As envisioned in the Order, the Framework generally contains "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber-risks."[200] This Framework was developed through consultation with critical infrastructure owners and operators, sector-specific federal agencies, and the National Security Agency (NSA) among others, and "shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[201]

As it currently stands, the Framework focuses on providing generalized overarching cybersecurity risk management principles for use in critical infrastructure, regardless of the sector, size, degree of cybersecurity risk faced or cybersecurity sophistication of the particular entity involved.[202] It emphasizes a process that assists individual entities in making informed business decisions on cybersecurity expenditures based on the likelihood of events occurring and resulting impacts.[203] Entities can determine for

---

[199] *See* Exec. Order No. 13,636, *supra* note 192, at § 7(e). *See generally* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY VERSION 1.0 (2014) [hereinafter NIST FRAMEWORK], *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[200] Exec. Order No. 13,636, *supra* note 192, at § 7(a).
[201] *Id.*
[202] NIST FRAMEWORK, *supra* note 199, at 1–2.
[203] *Id.* at 5.

themselves the acceptable business level of risk to their critical services and are allowed to handle it in a variety of ways, which include mitigation, transference, avoidance, or even simple acceptance.[204]

At least one cybersecurity commentator has stated that the Framework wrongly "encourages an actuarial approach to risk assessment" rather than a capabilities-based assessment which would evaluate enemy attack capabilities against defensive capabilities.[205] Because cybersecurity incidents historically have been small in number and cost, and to date relatively insignificant, increased cybersecurity investment will often lose to simple transference of risk (through purchase of insurance) or even just status quo acceptance.[206] If critical infrastructure owners and operators choose either of those courses of action when confronted with risk, then those that depend on those critical services are no better protected; it would likely take the occurrence of large scale crisis event to really cause owners and operators to seriously reevaluate the risk incidents against cybersecurity investment.

Additionally, since the standards are voluntary, the industry must have sufficient incentives to actually adopt the standards that are developed. This is particularly true for any standards developed regarding ICS, which can be exceedingly costly to replace, patch, or upgrade. Since there is no liability protection or tax incentives offered, there is little immediate upside, from a cost-benefit analysis standpoint, for the private

---

[204] *Id.*
[205] Lior Frenkel, *NIST Framework Misses the Mark on Risk Assessment*, WATERFALL (Dec. 26, 2013, 10:09 AM), http://waterfall-security.blogspot.com/2013/12/nist-framework-misses-mark-on-risk.html.
[206] *Id.*

industry to adopt any ICS changes that carry significant costs or reduce network connectivity, as significant efficiencies will be lost.

Finally, if future standards developed by the NIST and/or industry regarding Internet connectivity and ICS security are too minimal or generalized, they can actually do more harm than good. If the utilities simply strive to meet minimum prescribed standards, this might leave them more vulnerable as opposed to them considering and addressing their cybersecurity in a more introspective manner. In sum, the Order and NIST standards fall far short of solving the key critical infrastructure vulnerabilities highlighted earlier in this paper. At best, the Order amounts to what General Keith Alexander, the head of the U.S. Cyber Command, referred to as "only a down payment on what we need to address the threat."[207]

B. Making Information Sharing Work

Information sharing, done correctly, provides tremendous advantages in making critical infrastructure more cybersecure. As discussed above,[208] it has the potential to yield increased situational awareness across the board for government and private participants and allows pooling of resources and collaborative problem-solving in an era when cyber-attacks can strike multiple targets simultaneously. Additionally, information sharing, working as intended, allows

---

[207] Suzanne Choney, *New Rules for Cybersecurity? Obama's Executive Order Explained*, MSN CANADA (Feb. 14, 2013, 10:15 AM), http://news.ca.msn.com/top-stories/new-rules-for-cybersecurity-obamas-executive-order-explained.

[208] *See supra* Part III.A.

the government to make better-informed regulatory choices about what cybersecurity standards would best protect the nation's critical assets in the future. However, despite two decades of emphasis on voluntary information sharing and the implementation of different sharing programs, information sharing has not come close to achieving its goals.

i. Centralized Information Sharing

As discussed above,[209] the current information sharing environment for critical infrastructure is often duplicative, cumbersome, and confusing to utilize. Mission overlap by different agencies has led to a host of different sharing portals that often need to be individually searched for any applicable advisories, vulnerability information, and best practices. Establishing a single recognized information sharing body whose efforts are closely synced with government efforts will help mitigate the confusion and duplication will continue to dominate.

A new information sharing regime must find a way to address the legal barriers that currently impede information sharing without undermining the interests that drove the creation of those barriers in first place. These interests include the ECPA's protections of personal privacy or antitrust laws meant to prevent anticompetitive collusion among businesses. Any new sharing organization or regime also needs to assuage the private business concerns of the shared information exposing corporations to government regulatory action or lawsuits.

---

[209] *See supra* Part III.

A nongovernmental nonprofit clearinghouse organization can meet many of these requirements, and such an organization, the National Information Sharing Organization (NISO), was proposed in a subcommittee draft of H.R. 3674 before being removed from the final committee version.[210] The NISO was envisioned to be a one-stop focal point for both government and private entities by integrating all of the existing information from sharing and analysis efforts into a single portal for communication and collaboration.[211] The NISO would be overseen by an elected board, which would include representatives from the DHS and other agencies with significant cybersecurity missions and representatives from the private industry, including one from each of the several critical infrastructure sectors.[212]

In addition, much like the CDC, which was originally viewed as a model for cybersecurity information sharing, the NISO would also fulfill a leadership role and have a number of distinctive capabilities useful to both the government and industry. These distinctive capabilities include maintaining a common operating snapshot, a 24/7 help desk, and providing

---

[210] H.R. 3674, 112th Cong. § 241 (2011), *available at* http:// http://www.homeland.house.gov/sites/homeland.house.gov/files/Draft Legislative Proposal on Cybersecurity.pdf.

[211] *Id.*; HOUSE REPUBLICAN CYBERSECURITY TASK FORCE, RECOMMENDATIONS 10 (2011), *available at* http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf.

[212] H.R. 3674, *supra* note 210, at § 243 (stating that how the board members would be elected was to be left to the NISO through development of its own procedures but that the critical infrastructure sectors that would each have a mandatory seat on the board would include: banking and finance, communications, DIB, two for energy (one for the electricity subsector and one for the oil and natural gas subsector), health care/public health, and information technology).

its own information analysis and proactive techniques based on its aggregation of the information it was receiving.[213] Also, like the DIB ECS program, the NISO would be able to receive and disseminate classified information to its cleared members.[214] By offering distinct, real-time and actionable information, the NISO can become the "go to" organization for cyber-threat awareness, analogous to what the CDC is now for infectious diseases. [215]

To alleviate the privacy concerns of individuals, as well as businesses with regard to any proprietary information, the NISO can put in place procedures to sanitize such information before providing it to the government or private industry NISO members. A House Republican Task Force Report that preceded the draft legislation, H.R. 3674, proposed adding a privacy board to the entity to periodically audit the information being shared and ensure that the privacy standards are being upheld.[216]

There are also a number of operational benefits that can be derived from NISO operating outside of the government. By

---

[213] *Id.* § 242; *Hearing on Draft Legislative Proposal for Cybersecurity: Hearing before the H. Comm. of Homeland Sec., Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Techs.*, 112th Cong. (2011) [hereinafter *Testimony of Dr. Gregory E. Shannon*], *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony Shannon_0.pdf (testimony of Dr. Gregory E. Shannon, Chief Scientist for the CERT Program at The Software Eng'g Inst. at Carnegie Mellon Univ.) (testifying about the various ways that some of the broader concepts regarding the NISO can be expanded upon and how they might work in practice).

[214] H.R. 3674, *supra* note 210, at § 247.

[215] *Testimony of Dr. Gregory E. Shannon*, *supra* note 213, at 4.

[216] HOUSE REPUBLICAN CYBERSECURITY TASK FORCE, *supra* note 211, at 11.

providing a secure and noncompetitive collaboration portal, the NISO might free the private industry from the competitive withholding of information that may be currently hindering the ISAC information sharing.[217] The entity can also remain free from the bureaucratic quagmire of overlapping missions, mission dilution, and lack of autonomy that often plague government information sharing efforts.[218] Ultimately, the NISO, as a "third party honest broker," would have the ingredients it needs to build the trust and confidence in information sharing that has proven elusive from the fragmented approach currently being pursued by the government and industry.[219]

An example of how valuable the NISO might be in practice can be demonstrated through the handling of the Conficker worm problem in 2009. This malware used a Microsoft Windows flaw to infiltrate computers and shut down important security systems and products, among other harmful effects, before spreading itself to other computers.[220] Ultimately, the malware could have potentially been used as a "powerful offensive weapon for performing concerted information warfare attacks that could disrupt" not only large corporations or whole countries, but even the Internet itself.[221] Due to the advanced evolving nature and rapid spread of the

---

[217] *See supra* text accompanying note 88.
[218] *See supra* text accompanying note 125.
[219] *Testimony of Dr. Gregory E. Shannon*, *supra* note 213.
[220] THE RENDON GROUP, CONFICKER WORKING GROUP: LESSONS LEARNED ii (2011), *available at* http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.
[221] John Markoff, *Computer Experts Unite to Hunt Worm*, N.Y. TIMES, Mar. 19, 2009, *available at* http://www.nytimes.com/2009/03/19/technology/19worm.html.

malware, a collaborative effort was required to tackle the problem. In response, a working group from across law enforcement, academia, and the computer and security industries was hastily formed at an Internet Corporation for Assigned Names and Numbers (ICANN) meeting .[222] Through this unprecedented collaboration, the Conficker Working Group (CWG) as it became known, was successful in not only coming up with the means of slowing the spread of the malware but also ultimately in preventing its use in any other significant cyber-attack.[223]

While the CWG proved that communication and collaboration are powerful tools to use against cyber-threats, they also demonstrated that its "whack-a-mole" approach to cyber-threats has shortcomings that a permanent and centralized approach, like that of the NISO, can help alleviate. First, there was no existing collaborative infrastructure in place, so considerable time was spent at the outset establishing the group by finding and engaging people with the right combination of skills and capabilities before the problem could even begin to be addressed.[224] In addition to attempting to solve the problem immediately, a centralized organization can also provide a single formal doorway for engaging government resources, as opposed to the CWG's informal and various attempts at engagement, which led to large inconsistencies in government response and participation and ultimately delayed their participation with CWG.[225]

---

[222] THE RENDON GROUP, *supra* note 220, at 18–19.
[223] *Id.* at 31.
[224] *See id.* at 38–39; *Testimony of Dr. Gregory E. Shannon*, *supra* note 213, at 4.
[225] *See* THE RENDON GROUP, *supra* note 220, at 40.

An existing and centralized organization like the NISO can also provide organizational tools that the ad hoc CWG could not bring to bear. These include, among others, a dedicated project manager to assign tasks, allocate resources, and ensure goals are met, a public relations staff to provide appropriate information to the public, media, and ISPs, and administrative support and testing facilities to help keep the experts focused on the malware problem.[226] A centralized organization like the NISO can also provide a single secure malware data repository to draw from and add to for research purposes, eliminating struggles like CWG's to create and maintain such a repository on the fly.[227] Further, by leveraging its broad standing technical expertise and organizational tools, such an organization can replicate the successes of the CWG on a more global scale with even greater efficacy.

ii. Careful Tailoring of What Information is Shared

The use of shared information between the government and private industry needs to be carefully tailored or a number of reasons. One reason, as already highlighted, is to not preempt important laws regulating antitrust and privacy, among others, to the point of undermining the important purposes these laws serve. Defining too broadly what cybersecurity information will be shared and allowing the sharing of it "notwithstanding any law" will have the effect of running a bulldozer through other important societal values and will have adverse unintended effects.[228] Since the ultimate goal of

---

[226] *Testimony of Dr. Gregory E. Shannon*, *supra* note 213, at 4.
[227] *Id.* at 5.
[228] *Hearing on Draft Legislative Proposal for Cybersecurity: Hearing before the H. Comm. of Homeland Sec., Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Techs.*, 112th Cong. (2011) [hereinafter

sharing is to increase communication on threats and vulnerabilities in pursuit of stronger cybersecurity, there needs to be sufficient protections in place to foster that sharing environment. For there to be a free flow of information, private industry actors will need assurances that the shared information will not be the fuel for lawsuits or enforcement actions by regulatory agencies.

The discussion draft of the House Resolution did not define what cybersecurity information would actually be shared. However, the unenacted Cybersecurity Act of 2012 ("Act") does provide some useful definitions that can be drawn upon in that regard. Specifically, the Act uses the term "cybersecurity threat indicator" to describe the information that can be shared.[229] The definition includes information "reasonably necessary to describe" a host of listed techniques and methods by which cyber-intrusions might occur, such as malicious reconnaissance, methods of defeating technical or operational controls, technical vulnerabilities, malicious cyber-command and control, any actual or potential harm.[230] The definition only includes communication about any unlisted attribute of a cyber-threat, so long as the disclosure would not otherwise be illegal.[231] Finally, the definition also contains a privacy element. Entities can only share information "from which reasonable efforts have been made to remove

---

Testimony of Gregory T. Nojeim], *available at* https://cdt.org/files/pdfs/Cybersec_testimony_House_Homeland_Security.pdf (testimony of Gregory T. Nojeim, Director, Project on Freedom, Security & Technology, Center for Democracy & Technology).

[229] Cybersecurity Act of 2012, S. 2105, 112th Cong. § 708(6) (2012).

[230] *Id.* §§ 708(6)(A)(i)–(vii).

[231] *Id.* § 708(6)(A)(viii).

information that can be used to identify specific persons unrelated to the cybersecurity threat."[232]

This focused definition is beneficial for a number of reasons. First, from an operational standpoint, it helps the NISO by constraining the amount of information they are being fed from various sources to what they really need in the interests of cybersecurity. As a result, the NISO can analyze, aggregate, and re-share the information it receives as rapidly as possible without having to take extra time to filter out the non-useful information and sanitize sensitive privacy-related information on its own.

Second, the definition limits the number and breadth of laws that need to be preempted. Information that does not fall within the relatively narrow confines of the definition would not receive liability protection. This is of particular importance in the area of privacy, as the focus ensures that the only personally identifiable information that is shared is that which is crucial to respond to a cyber-threat.[233] The focused definition also meshes well with the authority already provided in the ECPA, which allows providers and other operators to intercept, use, and disclose information running through their networks for self-defense purposes. [234] Thus, disclosures to the

---

[232] *Id.* § 708(6)(B).

[233] MICHELLE RICHARDSON, AM. CIV. LIBERTIES UNION, INTERESTED PERSONS MEMO ON CYBERSECURITY INFORMATION SHARING LEGISLATION AND PRIVACY IMPLICATIONS IN 112TH CONGRESS 2 (2012), *available at* http://www.aclu.org/national-security-technology-and-liberty/aclu-interested-persons-memo-cybersecurity-information.

[234] *See* 18 U.S.C. § 2511(2)(a)(i) (2012) (allowing providers to intercept, use and disclose communications passing over their networks while they are engaged in "any activity which is a necessary incident to the rendition of his

NISO will merely extend that authority in the interest of defending others as well. While the Senate Bill fails to define what constitutes "reasonable efforts" to remove personal identification, those procedures can be developed by the NISO itself in conjunction with its reporting and privacy procedures.

Finally, for shared information that does qualify as a "cyber threat indicator," certain protections should apply to foster the information sharing environment. Such protections should include exemption from disclosure under the Freedom of Information Act,[235] prohibition on use in any civil action (without the consent of the submitter), and a prohibition on disclosure to government officers or employees except under defined circumstances.[236] A good definition of when the information might be disclosed to government officials was included in the SECURE IT Senate Bill ("Bill").[237] The Bill proposed that information can only be disclosed to the government for a cybersecurity or national security purpose, or to prevent, investigate, or prosecute crimes listed under 18 U.S.C. § 2516 for which a wiretap order may be sought.[238] Again, these exceptions mesh well with the existing exceptions in the law. For example, the ECPA already contains exceptions that allow for providing the government with information in

---

service or to the protection of the rights or property of the provider of that service).

[235] 5 U.S.C. § 552(b)(3) (2012). The Critical Infrastructure Protection Act, 6 U.S.C. §133 (2012), already exempted from disclosure information pertaining to actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by computer-based attack.

[236] H.R. 3674, *supra* note 210, at §§ 248(a)(1)–(3).

[237] SECURE IT, S. 3342, 112th Cong. (2012).

[238] *Id.* § 102(c)(1).

case of emergencies or for national security purposes.[239] These limitations are broad enough to ensure maximum utility for the government while also alleviating any fears of the private industry that the shared information might lead to a host of regulatory enforcement actions.

iii. Mandatory Information Sharing

Even after two decades, voluntary information sharing has failed to create an effective information sharing environment, so some kind of mandatory information sharing model for critical infrastructure may be the next step. In fact, mandatory reporting of incidents and vulnerabilities are not uncharted waters for critical infrastructure. In the energy sector, utilities have been mandated by law since the mid-1970s to report disturbance and emergency information to the Department of Energy (DoE) subject to triggering criterion and within the prescribed time limits.[240] For example, power plants currently have to file a Form OE-417 ("Form") with the DOE within one hour of a physical or cyber-attack that causes major interruptions in electrical system operations or within six hours if the event could potentially impact electric power system adequacy or reliability.[241] The Form requires submission of basic information (e.g., utility and area affected, dates, times, basic type of attack, etc.) to help the DOE track incidents from a national security standpoint. The information provided on an

---

[239] 18 U.S.C. §§ 2702(b)(8), (c)(4), 3125(a)(1) (2012).

[240] *See* Federal Energy Administration Act of 1974, 16 U.S.C § 761(a) (2012).

[241] *See* U.S. DEP'T OF ENERGY, FORM OE-417 (2012), *available at* http://www.eia.gov/survey/form/oe_417/instructions.pdf (instructing electricity providers to provide notice and supporting information to the DOE within one hour under eight distinct criteria and within six hours under four additional criteria).

OE-417 is relatively basic and would generally only translate to checking a single box on the Form in the case of a cyber-attack.

A similar mandate can be used to compel the reporting of cyber-attack information to an information sharing body regardless of whether the attack causes any negative effects on the service being provided. A potential good starting point might be the language drawn from the Cybersecurity and Internet Freedom Act of 2011.[242] This act mandates that "the owner or operator of covered critical infrastructure shall report any incident affecting the information infrastructure . . . to the extent the incident might indicate an actual or potential cyber risk, or exploitation of a cyber risk . . . ."[243]

Adopting a similar regulation may empower the NISO to fill out the specifics of the reporting requirement. Much like the power plant reporting to the DOE example, the actual content and timeliness requirements of the report should be developed by the NISO in accordance to its needs. Participation by the critical infrastructure will likely ensure that the reporting required is tailored to address the actual information needs of NISO. Additionally, the NISO's ability to protect the information it receives will likely make the private industry more willing to engage in some level of reporting.

Initial reports might first focus on the most basic information as it becomes known: the type of attack/threat, the source of the attack, the component targeted, andany effects on any systems. Follow-up requirements might include things

---

[242] S. 413, 112th Cong. (2011).
[243] *Id.* § 246(c)(1)(A)(i).

such as the particular cybersecurity vulnerability discovered from the attack and any lessons learned or best practices developed as a result. Setting modest requirements in the beginning may help build the trust and confidence in NISO that it ultimately needs to be successful.

C. Addressing Cyber-Insecure ICS

"Cyber is a three-legged stool[:] ease-of-use, security and privacy . . . . To date, almost all of our creative energies have been put into ease-of-use. . . . Like any three-legged stool, if you don't have all three legs, what you have is firewood."
- General Michael Hayden (Ret.)[244]

While information sharing is a vital part of any solution to the threats against critical infrastructure, it cannot, alone, form the foundation upon which future protection of those assets rests. Even the most intensive information sharing programs have only, at the end of the day, produced modest protective results on its own.

The best example of this in critical infrastructure practice is the DIB ECS program. The program, as touched on earlier in this Article,[245] provided defense contractors with classified and unclassified cyber-threat information as well as best practices in return for the contractors reporting cyber-incidents and coordinating mitigation strategies.[246] The DIB companies participating in the program believed that the program would prove that the NSA threat signatures can

---

[244] BAKER ET AL., *supra* note 19, at 15.
[245] *See supra* Part IV.A.
[246] *See* Exec. Order No. 13,636, *supra* note 192; FISCHER ET AL., *supra* note 193, at 6.

provide optimum protection, but a recent report on the program found that the goal was somewhat unrealized.[247] While the report found that the program employed information sharing successfully, many of the NSA "signatures" of malicious codes were "stale when deployed" and would not have helped the companies to prevent any intrusions that they could not have blocked on their own.[248] Ultimately, the original lofty goal of providing a optimum level of protection proved unattainable, and the goal of the program had to be scaled back to "a baseline level of protection."[249]

For critical infrastructure, the other component of a cybersecure foundation is addressing the current state of cyber-insecure ICS. Two decades of developing computer networks based on Internet connectivity have created sizable efficiencies and cost-savings for consumers and private companies that run a lot of the nation's critical infrastructure. Unfortunately, security technology and practices for ICSs have not kept pace, and the cost of bridging this gap is significant and does not currently feature into the corporate business plan. This is because from a corporation's point of view, investing in increased cybersecurity requires spending on nonproductive assets, which, by definition, will not generate increased profit return on any investment.[250] As a result, according to one

---

[247] Ellen Nakashima, *Cyber Defense Effort is Mixed, Study Finds*, WASH. POST, Jan. 12, 2013, *available at* http://articles.washingtonpost.com/2012-01-12/world/35438768_1_cyber-defense-nsa-data-defense-companies.
[248] *Id.*
[249] *Id.*
[250] *Examining the Cyber Threat to Critical Infrastructure and the American Economy: Hearing before the H. Comm. of Homeland Sec., Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Techs.*, 112th Cong. 42 (2011) (testimony of James A. Lewis, Director and Senior Fellow, Tech. and Pub. Policy Program, Ctr. for Strategic and Int'l Studies).

survey, cost is by far the largest obstacle to achieving better cybersecurity in most privately held critical infrastructure.[251] One power company CEO who decided to invest in cybersecurity might sleep better at night from a security perspective but would also see lost profits from customers choosing to buy electricity from cheaper sources. Thus, any solution to the insecure ICS problem has to weigh these costs and benefits.

One possible solution, making the government responsible for generating standards for private critical infrastructure, has already been discussed in reference to the voluntary "cybersecurity framework" put in place by the Order.[252] As discussed, it is highly doubtful that the NIST can develop thorough cybersecurity standards in a timely manner. There are simply too many different industries spread across a wide array of different sectors using distinct ICsS requiring specialized knowledge of those systems. Additionally, generalized standards, which will simply lead to compliance-ticking rather than a comprehensive cybersecurity approach, would probably do more harm than good. The Order also lacks the necessary incentives to get the private industry to actually adopt the developed practices.

An earlier White House legislative proposal, the Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act 2011, put forward a similar strategy but added mandatory compliance requirements and incentives that

---

[251] BAKER ET AL., *supra* note 19, at 14 (explaining that in the water/sewage and oil/gas sectors lack of awareness was cited ahead of cost, but the business case for cybersecurity was still a major challenge).
[252] *See* Part IV.A.

would have been available through legislation.[253] Basically, representatives from a wide array of organizations from each critical infrastructure sector, including the ISACs, sector coordinating councils, private industry, federal agencies with sector oversight, and state and local governments, would be invited to jointly develop a standardized cybersecurity framework for addressing vulnerabilities.[254] Then, the DHS, in consultation with the private sector, would evaluate the extent to which the proposed frameworks enhanced security in practice, specifically taking into account several stated factors.[255] If the sector framework proposed is found to be lacking based on those criteria, or no framework is submitted within one year, the NIST would be asked to develop that framework as discussed in the Order.[256] Based on the developed frameworks, the DHS would develop and enforce any additional regulations necessary to ensure that the framework-identified requirements were satisfied.[257]

Additionally, owners and operators of critical infrastructure would have to submit and annually certify compliance plans and be periodically evaluated by third-party

---

[253] *See* OFFICE OF MGMT. & BUDGET, CYBERSECURITY REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE ACT (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act.pdf.
[254] *Id.* § 4(b)(1).
[255] *Id.* § 4(b)(2) (listing the following evaluation factors to include whether the standards "reasonably address identified cybersecurity risks," are cost-effective and demonstrate prioritizing of efforts, emphasize outcome-based metrics for measuring performance as opposed to mere compliance implementation, and include practical performance evaluation testing).
[256] *Id.* § 4(b)(4).
[257] *Id.* § 9.

accredited auditors for compliance.[258] Compliance with the whole strategy would limit liability and potentially increase research and development.[259] A very similar proposal emerged from the Senate in the form of the Cybersecurity Act of 2012.[260]

While the Cybersecurity Act of 2012 wields greater "carrots" and "sticks" to try and jumpstart stronger cybersecurity standards, the process to achieve these standards is very cumbersome and time-consuming. Indeed, the involvement of each critical infrastructure sector in crafting a sector-specific cybersecurity framework would probably result in better, less-generalized standards for those sectors that produce a framework. However, if the sectors fail to produce a satisfactory plan as assessed by the DHS, or any plan at all, the NIST guideline development remains the fallback position. In addition, there is the follow-on process of the DHS and sector oversight agencies consulting with the private industry and determining what additional regulations are necessary in each sector. This approach is glacial and likely "far behind the technological curve of threats in cyberspace."[261] Thus, the entire strategy will most likely drive up costs and misdirect private industry resources without significantly increasing the cybersecurity of ICSs.

---

[258] *Id.* §§ 5–6.
[259] *See* OFFICE OF MGMT. & BUDGET, COMPLETE CYBERSECURITY PROPOSAL, §§ 243(c)(3), 246 (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.
[260] *See* Cybersecurity Act of 2012, S. 2105, 112th Cong. §§ 101–110 (2012).
[261] ROSENZWEIG, *supra* note 91, at 23.

A better approach would be to specifically target what private critical infrastructure mainly says is the largest obstacle: cost. In other words, the goal is to incentivize private critical infrastructure to make sustainable investments in cybersecurity that are not otherwise justified by their business plans. As discussed above,[262] the economic impact in order to achieve better ICS cybersecurity will be immense. There will be a substantial cost in developing new security technologies for ICSs to make them more secure and to replace older ICSs short of their normal life cycles. The industry will have to develop new methods of patching ICS software more expeditiously, which might mean adding redundant systems so that that ICSs can be taken offline to test patches. ICS cybersecurity training and certification programs will also have to be created, and more personnel will most likely have to be hired. Creating strong incentives for critical infrastructure expenditures in these areas is just one way to jumpstart better cybersecurity.

There are several ways the government can specifically create incentives for these programs. Some examples of such incentives include research and development tax credits or making grant funds available to purchase equipment and train personnel.[263] A role for the NIST, in conjunction with the NISO, if created, would be to endorse practices or standards that can qualify for these types of funds. Funds can also be

---

[262] *See supra* text accompanying notes 250–251.

[263] U.S. CHAMBER OF COMMERCE ET AL., IMPROVING OUR NATION'S CYBERSECURITY THROUGH THE PUBLIC–PRIVATE PARTNERSHIP 11 (2011), *available at* https://www.uschamber.com/sites/default/files/legacy/issues/defense/files/2011cybersecuritywhitepaper.pdf.

allocated for the research and development arm of the NISO itself. Over time, as the NISO's full analysis and aggregation capabilities are realized through information sharing, it will be able to leverage that informational wealth into promulgating cybersecurity best practices and baseline standards in each sector. The government can then craft cybersecurity regulations that can more effectively address emerging cyber-threats.

V. CONCLUSION

Warnings about the possibility of a "cyber–Pearl Harbor" are far from hyperbole. The critical infrastructure systems vital to the everyday operation of our government, economy, and well-being are already under attack, and trends indicate these attacks will continue to increase in number. The current state of cyber-vulnerability in critical infrastructure makes whether a component of critical infrastructure will be taken out not a matter of "if" but "when." Examples from government experiments to minor real-world examples demonstrate that such a takedown is possible. Further, because these vulnerabilities are prevalent in nearly every sector, there is a greater chance that several of these attacks can be chained together in such a way to cause destruction and death on a scale that can paralyze the nation.

Two vulnerabilities in particular stand out in need of addressing: insufficient information sharing and cyber-insecure ICS. Although the government and private critical infrastructure industry have focused on information sharing for two decades, a robust and effective system for sharing cybersecurity information still has not emerged. Legal barriers and government bureaucracy continue to hamper efforts in this regard. Additionally, the ICSs that run much of critical infrastructure have proven highly insecure in an era of added network and Internet connectivity. The private industry has

connected these systems to promote efficiency but often without mediating the great cybersecurity risk this creates.

A foundation of stronger cybersecurity for critical infrastructure can be laid by addressing these vulnerabilities. Centralization of government and private sharing efforts and some modest cyber-reporting requirements hold the keys for yielding the level of situational awareness and collaboration necessary to respond effectively in an era of cyber-attacks. Additionally, careful tailoring of what information is shared can ensure minimal preemption so that privacy and other important but nonessential societal norms are not undermined in the process.

Regarding ICS insecurity, the government is not best positioned to dictate ICS cybersecurity standards to private critical infrastructure. Generalized government standards will lead to even greater insecurity while sector-specific developed regulations are too time-consuming to develop. Rather, the role of the government should be to help the private industry overcome cost barriers in order to improve ICS cybersecurity through a centralization of efforts and providing a menu of strong incentives. On the other hand, owners and operators are best positioned to select measures from an incentive menu that will best secure their systems going forward.

Cybersecurity for critical infrastructure will grow stronger based on a foundation built on those elements. Centralized information sharing can ultimately provide the data needed to better inform private industry priorities and government regulation if needed. Incentive programs will jumpstart innovation and constitute a down payment on better ICS cybersecurity from the moment of creation rather than a backwards-looking process of regulation that can take months or even years to promulgate, thereby potentially making the

regulation stale upon being deployed. The nation needs real-time situational awareness and innovative cybersecurity standards to keep up with the technological curve of cyber-threats that confront critical infrastructure.