Florida State University Law Review

Volume 44
Issue 2 *Winter 2017*

Article 3

Winter 2017

Cybersecurity for Infrastructure: A Critical Analysis

Eldar Haber
University of Haifa

Tal Zarsky
University of Haifa

CYBERSECURITY FOR INFRASTRUCTURE: A CRITICAL ANALYSIS

ELDAR HABER* AND TAL ZARSKY**

ABSTRACT

Nations and their citizens rely on infrastructures. Their incapacitation or destruction could prevent nations from protecting themselves from threats, cause substantial economic harm, and even result in the loss of life. Therefore, safeguarding these infrastructures is an obvious strategic task for any sovereign state. While the need to protect critical infrastructures (CIs) is far from novel, digitization brings new challenges as well as increased cyber-risks. This need is self-evident; yet, the optimal policy regime is debatable. The United States and other nations have thus far opted for very light regulation, merely encouraging voluntary steps while choosing to intervene only in a handful of sectors. Over the past few years, several novel laws and regulations addressing this emerging issue have been legislated. Yet, the overall trajectory of limited regulatory intervention has not changed. With that, the wisdom of such a limited regulatory framework must be revisited and possibly reconsidered. This Article fills an important gap in the legal literature by contributing to and promoting this debate on cyber-risk regulation of CIs, while mapping out the relevant rights, options, and interests this 'critical' debate entails and setting forth a regulatory blueprint that balances the relevant factors and considerations.

The Article begins in Part II by defining CIs and cyber risks and explaining why cyber risk requires a reassessment of CI protection strategies. Part III describes the means used by the United States and several other nations to address cyber risks of CIs. Part IV examines a market-based approach with minimal governmental intervention to critical infrastructure cyber-regulation, along with the various market failures, highlighting assorted minimal measures to correct these problems. It further examines these limited forms of regulation, which merely strive to bridge information and expertise barriers, assign ex post liability for security-related harms, or provide other specific incentives—and finds them all insufficient. Part V continues the normative evaluation of CI cyber-protection models, focusing on ex ante approaches, which require more intrusive government involvement in terms of setting and enforcing standards. It discusses several concerns with this regulatory strategy, including the lack of governmental expertise, regulatory capture, compromised rights, lack of transparency, and the centralization of authority. Finally, in Part VI, the Article proposes a blueprint for CI cyber protection that goes beyond the mere voluntary regulatory strategy applied today.

* Senior Lecturer, University of Haifa, Faculty of Law; Haifa Center for Law and Technology, University of Haifa, Faculty of Law; Faculty Associate, Berkman-Klein Center for Internet & Society, Harvard University.

** Vice Dean and Professor, University of Haifa, Faculty of Law; Haifa Center for Law and Technology, University of Haifa, Faculty of Law.

We thank Derek Bambauer, Michael Birnhack, Courtney Bowman, Deb Housen Coureil, Haim Ravia, Ido Sevilla, Gabi Siboni, Lior Tabansky, Isabel Skierka, Gilad Yadin, Sharon Yadin and the participants of the "Algorithmic State: Cyber Challenges to Democracy and Civil Rights" conference for their thoughtful comments, Jordan Scheyer for her assistance in research, and Michele Manspeizer and Joshua Pens for their editing assistance.

I. INTRODUCTION

Nations and their citizens rely on infrastructures. Modern societies depend on electricity and transportation systems, banking and telecommunications, postal and shipping, and a variety of additional services that enable modern life and allow humanity to flourish.[1] Disruption of such services could cause annoyance, inconvenience, and financial losses to civilians, companies, and governments. Incapacitation or even destruction of infrastructures could result in more than mere inconvenience. It could eliminate nations' abilities to protect themselves from both domestic and foreign threats, cause substantial economic harm, lead to social unrest, and even result in loss of life. Therefore, protecting these infrastructures—especially those deemed critical—is an obvious strategic task and even duty of any sovereign state.

While the need to protect critical infrastructures (CIs) is far from novel, digitization brings about new challenges. In the pre-digital world, the government's role in protecting infrastructures was relatively justifiable and straightforward, as risks both originated and materialized in the kinetic realm. Thus, government and the relevant public and private entities[2] that controlled the infrastructures could focus on ensuring physical security by improving their resilience

1. BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES, at ix (2012) ("We depend heavily on shared infrastructures, yet it is difficult to appreciate just how much.").

2. In the United States, much of the CI is privately owned. For more on privatization of infrastructures in the United States, see Ellen Dannin, *Crumbling Infrastructure, Crumbling Democracy: Infrastructure Privatization Contracts and Their Effects on State and Local Governance*, 6 NW. J.L. & SOC. POL'Y 47 (2011).

against harms and by investing in protective and defensive measures from these well-known (if not predictable) risks.

The rise of the digital age substantially changes and realigns the threats CIs face and the forms of responses needed. CIs now rely on digital systems, such as Supervisory Control and Data Acquisition (SCADA)[3] operations. In some cases, these systems feature remote access and even control CIs. These and other technologies used for the monitoring and operation of CIs surely improve their functionality and generate vast social utility. Yet, employing digital measures expose CIs—and thus the state and society in general—to increased risks: risks of the *cyber* realm.[4] Such threats can materialize with both digital- and kinetic-related outcomes. In other words, they could manifest in the loss of data, the breakdown of a computerized system, or even the malfunction of electric grids, train systems, or sewage plants. Protecting CIs from cyber threats is therefore a substantial challenge of critical importance that is making its way from the desks of worried bureaucrats and policymakers to the mainstream press and public at large.

While the need to protect CIs from cyber risks is obvious, the optimal policy regime for achieving it is not. The United States and some other nations have thus far opted for very light regulation, merely encouraging voluntary steps while choosing to only intervene in a handful of sectors considered decidedly 'critical.' Yet the wisdom of applying a limited regulatory framework is currently under debate in the United States and worldwide. As the policy debate unfolds across the globe, a critical analysis of this timely issue and the delicate balance it involves is currently missing from legal academic literature. This Article intends to fill this gap, while mapping out the relevant rights, options, and interests this critical debate entails.

The Article proceeds as follows: Part II attends to the conceptual building blocks essential for the discussion to follow. It explains how the subsequent analysis defines CIs and cyber (as opposed to other) risks and discusses responses to date. It further argues that the digital age has brought about a new form of risk that requires reassessing CI protection strategies. Part III describes the current means used to govern and address cyber risks to CIs. It demonstrates that the United States has, thus far, generally relied on a 'hands off' approach (with some notable exceptions), merely generating frameworks for data sharing and voluntary standards for the private entities involved. This response differs from that of other countries, which set forth more in-

3. *See infra* note 15.

4. *See, e.g.*, JAYSON M. SPADE, INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 26 (Jeffrey L. Caton ed., 2012), https://permanent.access.gpo.gov/gpo30152/ChinasCyberPowerandAmericasNationalSecurity.pdf [https://perma.cc/SA9E-7WGG] (arguing that "a full scale critical infrastructure cyber attack could cost $700 billion").

trusive regulatory regimes that do not shy away from setting mandatory requirements for CIs—even when privately owned. Part IV begins the analytic search for an optimal form of regulation to assure protection of CIs from cyber threats. This Part starts by examining a market-based approach with minimal government intervention. While pointing out the shortcomings of such a minimalistic approach, this discussion highlights various measures to correct this type of regulation. In addition, this Part further examines limited forms of regulation that merely strive to correct information and expertise barriers, assign ex post liability for security-related harms, or provide other specific incentives. This Part normatively evaluates these models, concluding that on their own, they are insufficient to optimally protect CIs.

Part V continues the normative evaluation of CI protection models, focusing on ex ante approaches that require more intrusive government involvement through setting and enforcing standards. This Part discusses the benefits and drawbacks of these approaches, noting that they could, to a great extent, protect CIs. They also raise several concerns, however, including insufficient government expertise, regulatory capture, compromised rights, lack of transparency, and centralization of authority. Finally, in Part VI, after discussing existing CI protection models, this Article presents a proposed blueprint for CI cyber protection that accounts for and balances the various benefits and concerns set forth herein. This Article argues that regulators cannot take risks to CI lightly, but at the same time, suggests the implementation of measures that are consistent with civil liberties and tailored to the relevant threats and technologies. The Article concludes by noting the academic and regulatory challenges that remain to be resolved regarding this critical issue at hand.

II. PROTECTING (DIGITAL) CRITICAL INFRASTRUCTURE

A. Conceptual Building Blocks: CIs, Cyber (and Other) Risks, Outcomes, and Responses

Before examining and critiquing the policy landscape of CI cyber protection, a broad set of terms, motivations, and taxonomies must be introduced. First, what types of infrastructures are considered critical? Second, what forms of risks, both old and (more importantly) new, do they face? Third, what sort of negative outcomes could unfold, and consequentially, which responses are relevant? We address these basic questions in turn.

First, we must determine what renders an infrastructure critical, noting the importance of proceeding cautiously with this task. Too broad of a definition would place an economic burden on private corporations, government, and thus consumers, and taxpayers. But too narrow of a definition would exclude truly critical infrastructures from

regulatory schemes and lead to vulnerabilities, costs, and possible catastrophic outcomes. Originally, the U.S. regulatory framework defined CIs to include any infrastructure that "prolonged disruptions [which] could cause significant military and economic dislocation."[5] The White House, in Executive Order 13,010, broadened the definition to include "[c]ertain national infrastructures . . . so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[6] In 1998, under Presidential Decision Directive #63 (PDD-63), CIs were construed as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[7] Thus, toward the end of the previous century, the United States established two criteria for CIs: national defense and economic security.

Over time, and post 9/11, the United States added two additional criteria: public health and safety and national morale.[8] The national morale categorization was mostly used for CIs that were "national monuments and icons," as determined by the Department of Homeland Security (DHS) in its 2002 report.[9] However at a later stage, national morale CIs were reclassified as mere "key assets."[10] Thus, only three categories—national defense, economic security, and public health and safety—are included in the current U.S. CI framework.[11] While other countries use different definitions, this Article relies on this formal definition employed by the United States.

---

5. JOHN MOTEFF ET AL., CONG. RESEARCH SERV., RL31556, CRITICAL INFRASTRUCTURES: WHAT MAKES AN INFRASTRUCTURE CRITICAL? sum. (2003).

6. Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 17, 1996); *see also* MOTEFF ET AL., *supra* note 5, at CRS-5. Executive Order 13,010 included the following infrastructures: "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services . . ., and continuity of government." Exec. Order No. 13,010, 61 Fed. Reg. 37,347, 37,347 (July 17, 1996).

7. EXEC. OFFICE OF THE PRESIDENT, PRESIDENTIAL DECISION DIRECTIVE/NSC-63, CRITICAL INFRASTRUCTURE PROTECTION 1 (1998) [hereinafter CLINTON POLICY]; *see also* MOTEFF ET AL., *supra* note 5, at CRS-7.

8. MOTEFF ET AL., *supra* note 5, at CRS-16.

9. *See* PRESIDENT GEORGE W. BUSH, THE DEPARTMENT OF HOMELAND SECURITY 15 (2002), https://www.dhs.gov/xlibrary/assets/book.pdf [https://perma.cc/69BN-QLVX].

10. *See* OFFICE OF HOMELAND SEC., NATIONAL STRATEGY FOR HOMELAND SECURITY 30 (2002), https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf [https://perma.cc/PD36-EJZK]. Key assets are "individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our nation's morale and confidence." MOTEFF ET AL., *supra* note 5, at CRS-8.

11. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 § 1016, 42 U.S.C. § 5195(e) (2012). A similar definition of critical infrastructure first appeared in 2000 under a National Plan for Critical Infrastructure. *See* EXEC. OFFICE OF THE PRESIDENT, DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION VERSION 1.0: AN INVITATION TO A DIALOGUE iii (2000), https://fas.org/irp/offdocs/pdd/CIP-plan.pdf [https://perma.cc/3QR6-F4KQ].

It is important before proceeding to note the relationship between cyber attacks and CIs. Although cyber attacks seemingly take place in the cyber world, they cause physical, real, and non-cyber harms and damages. Thus, protecting CIs could take on a multitude of forms (cyber and/or physical-kinetic). While this Article is concerned with cyber attacks and risks, both the outcomes and countering measures are closely tied to the physical/kinetic world. Accordingly, the short discussion in the following paragraphs strives to explain the focus of this Article and, more specifically, the relationship between cyber and physical/kinetic elements.

Cyber risks might materialize on several levels. Comparatively, analog world risks generally threaten physical infrastructures, or at least, damage to areas in close proximity to them. Thus, in addition to intelligence gathering, fears of analog world risks can usually be mitigated by creating physical barriers and perimeters. Physical security of this sort is, of course, essential to discourage cyber risks as well. IT infrastructures face physical attacks or direct computer access with the intention to damage the CI. Yet as this Article explains below, CIs can also be harmed through remote digital access—i.e., the saboteur has no need to be in the area. Thus, decreasing cyber attacks on CIs calls for an additional set of protective measures.

Moreover, the prospect of cyber attacks against CIs introduces a specific subset of outcomes and risks that is discussed throughout this analysis. In a purely analog world (one without central IT systems in CI operations), system damage and destruction constitute the main risks to CIs. While relevant in the cyber realm as well, these risks and outcomes are joined by additional ones, such as information theft (including personal data) and unwanted data alteration. Although these novel risks might not seem as severe, they do require a different set of measures and responses—ones with which regulators are currently grappling.

B. Cyber Attacks: A Growing Threat that Calls for a Response

The intentional actions of human adversaries as part of armed or unarmed conflicts between nations, criminal activities (including various types of hacking), revengeful measures of disgruntled employees, or acts of terrorism pose a substantial threat to CIs. CIs—both at a physical and digital level—also face the same risks as a result of unintentional actions, such as human error, poor design, and even natural causes.[12] While these latter issues are not discussed

12. JOHN D. MOTEFF, CONG. RESEARCH SERV., RL30153, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION 1 (2015), https://www.hsdl.org/?view&did=767176 [https://perma.cc/2877-BVJM].

in the following analysis, many of the points made in the subsequent Parts herein pertain to them as well.

There are several convincing reasons to believe that CIs are generally attractive targets.[13] First, CI targets are numerous and spread out, rendering them vulnerable. Second, CIs are, in many cases, interdependent. Disruptions caused to one sector could have repercussions across many others. For instance, an attack against a country's power grid could negatively affect transportation, communications, and emergency service infrastructures. Third, attacks against CIs could have a powerful psychological effect on society. Therefore, adversaries have a publicity incentive to attack them and enhance their visibility and prestige. Fourth, due to a variety of market failures, private CI owners may under-invest in security measures and lack necessary intelligence on impending attacks.

While the risks noted above might seem sufficient motivation for a regulatory-based discussion, some may argue these risks have already been sufficiently mitigated in the existing equilibrium between state regulation, public pressure, and market forces. This might be true. Yet the increase in cyber risks and their associated outcomes alters the status quo and demands urgent re-examination of the issue at hand. To illustrate this point, we consider the existing analytical paradigm used by the DHS to assess CI's risks.

In its efforts to formulate a balanced and appropriate defense, and to ensure that the risks to CI facilities and security measures are matched appropriately, the DHS Risk-Based Performance Standards identified three factors that indicate a security risk: (1) likelihood of a successful attack (*vulnerability*); (2) existence of an adversary with the necessary intent and capabilities to attack the facility (*threat*); and (3) consequences of a successful attack on a facility (*consequence*).[14] This Article uses the DHS Risk factors and explores the impact of digitization on them. This inquiry shows that the growing presence of 'cyber' elements calls for reconsideration, and possibly readjustment, of the CI's cyber protection strategy.

Digitization, cyber and *vulnerability*. The move toward digitization within CIs has increased dependency on technology, which, in turn, may have reduced some of the existing threats, especially those associated with human negligence. However, this move may have also in-

13. For some of these reasons, see Joe D. Whitley et al., *Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection*, 47 JURIMETRICS 259, 268-73 (2007).

14. *See* RISK STEERING COMM., DEP'T. OF HOMELAND SEC., DHS RISK LEXICON 17, 30 (2008), https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf [https://perma.cc/9XML-8Y6X].

creased vulnerability, or at least generated new forms of it. To demonstrate, note that CI operators use SCADA systems,[15] as well as other computers and networks,[16] to monitor and control CI systems. Moreover, CIs are often networked and even connected to the Internet,[17] which too generates a novel set of vulnerabilities[18] as now attacks can be launched remotely.[19] At times, CIs might be interconnected among themselves. In some cases, this form of vulnerability is compounded by the fact that such technology and equipment may be of foreign origin and therefore prone to abuse.[20] CIs' vulnerability further increases because cyber attacks can be ongoing and are adaptable, which increases their likelihood of success.[21]

Scope of Cyber *Threat*: Resources and Location. Let us begin with an intuitive, yet questionable, assumption—cyber attacks are less expensive to execute than physical attacks. If this is indeed the case, the possibility of cyber attacks exacerbates the threats CIs face today. But we must be cautious of this generalization. Not every cyber attack comes cheap,[22] especially not sophisticated ones. Consider the alleged

---

15. "SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation." NAT'L COMMC'NS SYS., TECH. INFO. BULLETIN 04-1, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS 4 (2004), https://scadahacker.com/library/Documents/ICS_Basics/SCADA%20Basics%20-%20NCS%20TIB%2004-1.pdf [https://perma.cc/JW3X-FB4N].

16. Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 407 (2007) ("Networked computer systems form the nerve center of the country's critical infrastructure.").

17. *See* Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor,"* 18 VA. J.L. & TECH. 289, 302-03 (2014).

18. Gareth Evans, *Protecting Critical Infrastructure in the Digital Age*, ARMY-TECHNOLOGY.COM (Feb. 14, 2012), http://www.army-technology.com/features/featureprotecting-critical-infrastructure-in-the-digital-age [https://perma.cc/AJ9P-JFT3] ("For centuries CIP simply involved ensuring that your enemy did not physically destroy [your CIs], nor take control of them away from you by force. In the digital age, however, things have become more complex, as conflict has gone online - and the potential implications for CIP are enormous.").

19. For more on the potential vulnerabilities of SCADA, see Rodrigo Chandia et al., *Security Strategies for SCADA Networks*, *in* CRITICAL INFRASTRUCTURE PROTECTION 117 (E. Goetz & S. Shenoi eds., 2008).

20. Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch— The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 307-09 (2008) (listing vulnerabilities in the "cyber battlefield").

21. *See, e.g.*, Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 618 (2011) [hereinafter Bambauer, *Conundrum*].

22. One study suggested that it would take "thirty hackers with a budget of $10 million [to] bring the United States to its knees." *See* Scott Dynes et al., *Cyber Security: Are Economic Incentives Adequate?*, *in* CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 19, at 15.

use of the 'Stuxnet' computer worm to attack Iran's uranium enrichment centrifuges.[23] Stuxnet was a highly sophisticated weapon, which required substantial manpower and expertise to create.[24] It was especially tailored for a very specific computer system as well as for stealth activation and operation. If this example is indicative, cyber attacks might be just as costly and difficult to execute as physical ones, if not more.

But not all cyber attacks aspire to meet the high 'Stuxnet' standard. There are other forms of cyber attacks that are neither sophisticated nor expensive. Cyber attacks can be deployed by exploiting unsophisticated technological vulnerabilities without using substantive human or economic resources. In fact, information on 'how to execute a cyber attack' is widely available online for free, as are free or cheap exploitation tools.[25] Whether these types of attacks constitute a strategic risk to, or a mere nuisance for, CIs is currently unclear. That said, there is a chance that these cheap, easy attacks will cause real damage at least to a negligent CI and should thus be considered an enhanced threat.

The prospect of cyber attacks on CIs also broadens the pool of potential attackers, again enhancing the threat. Unlike many physical attacks, cyber attacks will not immediately threaten the life of the attacker when carried out remotely. Therefore, cyber terrorists are less restricted than terrorists in the kinetic world and can attack multiple targets. Cyber attacks might attract an entirely new set of adversaries; rather than driven terrorists, they might be launched by teenage hackers who might be strongly deterred by attacking armed guards but lack such hesitation in their parents' basement.

Law enforcement faces a variety of enforcement difficulties, particularly in locating the online criminal. Cyber attacks can occur beyond the sovereignty of the state, so the culprit does not need to escape and thus has fewer risks. Cyber attacks also raise an 'attribution problem.'[26] Attackers use digital technology to cover their tracks or even

---

23. Michael B. Kelley, *The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, BUS. INSIDER (Nov. 20, 2013, 12:58 PM), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T [https://perma.cc/X5QZ-S5FZ].

24. *See* Bruce Schneier, *The Story Behind the Stuxnet Virus*, FORBES (Oct. 7, 2010, 6:00 AM), http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html [https://perma.cc/H4EY-5FK5].

25. *See* Solce, *supra* note 20, at 307-09 (listing vulnerabilities in the "cyber battlefield").

26. COMPUT. SCI. & TELECOMMS. BD., NAT'L RESEARCH COUNCIL, CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 4 n.9 (2002), http://citadel-information.com/wp-content/uploads/2012/08/cybersecurity-today-and-tomorrow-pay-now-or-pay-later-national-research-council-2002.pdf [https://perma.cc/W7HT-LFLG] ("Tracing attacks is generally difficult, because serious attackers are likely to launder their connections to the target. That is, an attacker will compromise some intermediate targets whose vulnerabilities are easy to find and exploit, and use them to launch more serious attacks on

implant false and deceptive identification marks. In many instances, the attacker's true identity is protected because she used a public or 'zombie' computer belonging to another.[27] All of these elements minimize the chances of attackers getting caught, thus improving the attackers' capabilities to attack and enhancing the threat of their actions.

The cyber realm also enhances the accessibility of threatening tools and measures. Equipped with the correct set of skills, almost anyone, from any place, can execute an attack, using even public computers. Contrast this with physical attacks, which usually require purchasing or concocting explosives or other weapons, which are not as widely available as computers. Furthermore, digital weapons can usually be purchased on black markets[28] and attacks ordered via more secured communications. Cyber conditions therefore increase the set of potential attackers and thus the threats they generate.

Difficulty of Detection and *Consequences*. As is previously noted, cyber attacks are often difficult and expensive to detect and attribute to one specific attacker. These factors render such attacks more dangerous, as their outcomes could be dire for several reasons. Cyber attacks—as opposed to kinetic destruction—could remain undetected for an extensive period of time.[29] The passage of time allows the attacker to cause even greater harm.[30] Furthermore, when intrusion into the CI remains undetected, the attacker can execute the attack at any time—usually the point at which the greatest damage will be caused. Finally, the attack might never be detected if the damage and disruption it caused is

---

the ultimate intended target."). For more on the attribution problem, see, e.g., David D. Clark & Susan Landau, Essay, *Untangling Attribution*, 2 HARV. NAT'L SECURITY J. 323, 326 (2011); Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 A.F.L. REV. 1, 31 (2009) (arguing that it might be difficult to attribute cyber attacks without the assistance of the country of origin); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1538 (2010); Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 984-93 (2011).

27. A good example is a distributed denial of service (DDoS) attack, in which a virus compromises an end user computer and the attacker hijacks their computer to flood a target with too much data for it to handle. Therefore, the target views the end-user as the attacker, while the true attacker controls the end user's actions. For more on DDoS attacks and legal responsibility, see Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23 (2006).

28. *See* Solce, *supra* note 20, at 307 (mentioning the existence of "black market[s]" which sell information on computer vulnerabilities in the "cyber battlefield").

29. *See* PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 18 (1997), http://chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf [https://perma.cc/4QR5-AXFJ] ("Computer intrusions do not announce their presence the way a bomb does. . . . It sometimes takes months, even years, to determine the significance of individual computer attacks.").

30. An example is the usage of the previously mentioned computer worm "Stuxnet," which took a long time to discover. *See* Kelley, *supra* note 23.

attributed to a malfunction. This oversight allows the attackers to repeat their actions at a later time, causing even greater harm.

To summarize this Section, we note that the cyber era brought about many improvements and benefits to CIs. But at the same time, this era requires reassessing the management and defense of CIs. Cyber attacks can be simple to execute, quick, anonymous, accessible, and more affordable than physical attacks. Their implications can be more profound than physical attacks. What some commentators refer to as a "cyber" or "electronic Pearl Harbor"[31] could have devastating consequences on the economy of any nation and its citizens.[32] Therefore, the regulation of such risks—on a practical, strategic, and theoretical level—must be reconsidered.

III. APPROACHES TO CRITICAL INFRASTRUCTURE PROTECTION

A. The U.S. Approach

1. The Rule: Limited Intervention

The United States has been responding to and regulating cyber risks to CIs for over two decades. The U.S. strategy shows a clear direction—one of limited intervention in the action of private CIs. Several very different administrations—each faced with varied challenges and external events—have embraced this strategy, even after numerous chances to amend it. Nonetheless, more layers have been added to the regulation over the past few years, which have allowed for more meaningful guidance from government as well as facilitated information sharing regarding this complex threat. This Article uses a chronological review (rather than a grouping of similar issues) to convey a sense of how these matters have dynamically unfolded.[33]

The Clinton Administration—Acknowledgment and Foundations: The United States first acknowledged the importance of protecting CIs in the aftermath of the Oklahoma City bombing in April 1995, but its

---

31. MYRIAM DUNN CAVELTY, CYBER-SECURITY AND THREAT POLITICS: US EFFORTS TO SECURE THE INFORMATION AGE 91 (2008); *see also Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor*, FOREIGN POLICY (Apr. 2, 2008), http://foreignpolicy.com/2008/04/02/seven-questions-richard-clarke-on-the-next-cyber-pearl-harbor/ [https://perma.cc/6UCZ-G2KH].

32. *See, e.g.*, William C. Banks & Elizabeth Rindskopf Parker, Symposium, *Introduction*, 4 J. NAT'L SECURITY L. & POL'Y 7, 9-11 (2010); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U.L. REV. 1503, 1505 (2013).

33. For a similar review method, see Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, MICH. ST. L. REV. 1475, 1520-23 (2014).

response was measured.[34] President Clinton created an inter-agency Critical Infrastructure Working Group (CIWG) to study the infrastructural vulnerabilities of the United States and provide recommendations. CIWG's recommendations, announced in March 1996,[35] led to the formation of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996.[36] PCCIP released a report in October 1997[37] finding "no immediate crisis threatening the nation's infrastructures," but simultaneously finding reason to take action on cybersecurity.[38] Eventually, in May 1998, the PCCIP's report led to two Presidential Decision Directives: PDD-62 and PDD-63.[39]

PDD-63 identified the importance of increasing public awareness of critical infrastructure and named achieving protection of the nation's CIs by the year 2003 as a national goal.[40] To accomplish this, PDD-63 identified which services needed protection[41] and determined which federal agencies would take the lead in four government functions: "internal security and federal law enforcement; foreign intelligence; foreign affairs; and national defense."[42] Lead agencies were responsible for coordinating cooperation with private sector organizations, which were encouraged to collaborate. The Presidential Decision Directives also established new federal entities—notably, the National Infra-

34. CAVELTY, *supra* note 31, at 91; Eric A. Greenwald, *History Repeats Itself: The 60-Day Cyberspace Policy Review in Context*, 4 J. NAT'L SECURITY L. & POL'Y 41, 43 (2010).

35. The working group made two proposals: First, to create "a full-time Task Force in the Executive Office of the President to study infrastructure assurance issues and recommend national policy." Memorandum from Janet Reno, Att'y Gen., to Robert E. Rubin, Sec'y of the Treasury, et al. (Mar. 14, 1996) (http://fas.org/sgp/othergov/munromem.htm [https://perma.cc/6AZ9-APLK]) (memorandum on Critical Infrastructure Security). Second, to establish "a single interagency coordinating group within the Department of Justice, chaired by the FBI, to handle the interim infrastructure assurance mission with regard to both physical and cyber threats and to coordinate the work of the government in this area." *Id.*

36. Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 17, 1996).

37. PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., *supra* note 29.

38. MOTEFF, *supra* note 12, at 3.

39. EXEC. OFFICE OF THE PRESIDENT, PROTECTION AGAINST UNCONVENTIONAL THREATS TO THE HOMELAND AND AMERICANS OVERSEAS: PRESIDENTIAL DECISION DIRECTIVE/NSC-62 (1998); CLINTON POLICY, *supra* note 7; *see also* CAVELTY, *supra* note 31, at 91.

40. *See* CLINTON POLICY, *supra* note 7, at 2; MOTEFF, *supra* note 12, at 4.

41. "[I]nformation and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power; oil and gas production, and storage." MOTEFF, *supra* note 12, at 4 (citing CLINTON POLICY, *supra* note 7, at 10).

42. *Id.* (citing CLINTON POLICY, *supra* note 7, at 10).

structure Advisory Council (NIAC), the National Infrastructure Protection Center (NIPC), and the Critical Infrastructure Assurance Office (CIAO).[43]

The Bush Administration—Institution Building: In the aftermath of 9/11, the organizational framework of agencies and institutions responsible for protecting CIs was somewhat revised, yet the overall strategy remained constant. The main change during this time was the establishment of new institutions. On October 8, 2001, President Bush signed Executive Order 13,228, establishing the Office of Homeland Security[44] and the Homeland Security Council.[45] On October 16, 2001, he signed Executive Order 13,231, which created the President's Critical Infrastructure Protection Board and the National Infrastructure Advisory Council.[46]

In 2002, Congress created the Department of Homeland Security (DHS), to which many of the above-noted responsibilities related to the protection of CIs eventually gravitated.[47] The Secretary of Homeland Security replaced the National Coordinator as the nation's cyber coordinator.[48] In addition, many agencies and offices—including the National Infrastructure Protection Center (NIPC) and the Critical Infrastructure Assurance Office (CIAO)—were incorporated into the DHS.[49]

---

43. NIAC was created to "provide the President through the Secretary of Homeland Security with advice on the security of the critical infrastructure sectors and their information systems." *National Infrastructure Advisory Council*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/national-infrastructure-advisory-council [https://perma.cc/53ZX-L528]. NIPC was created to "serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity," CLINTON POLICY, *supra* note 7, at 12, and received operational responsibilities and was located within the Federal Bureau of Investigation (FBI). Greenwald, *supra* note 34, at 49. CIAO was formed in the Department of Commerce, designed "to coordinate the development of a public-private partnership . . . . " *Id.*

44. The Office of Homeland Security was tasked "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 10, 2001); MOTEFF, *supra* note 12, at 8 (citation omitted).

45. MOTEFF, *supra* note 12, at 8-9.

46. Exec. Order. No. 13,231, 66 Fed. Reg. 53,063 (Oct. 18, 2001). The President's Critical Infrastructure Protection Board "was authorized to 'recommend policies and coordinate programs for protecting information systems for critical infrastructure.' " MOTEFF, *supra* note 12, at 9 (citation omitted). The National Infrastructure Advisory Council's main task was to advise the President "on the security of information systems for critical infrastructure." *Id.*

47. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

48. Greenwald, *supra* note 34, at 49.

49. *Id.* at 50. The Act also transferred other agencies and offices which are related to critical infrastructure protection, e.g., the Federal Computer Incident Response Center (FedCIRC), the National Infrastructure Simulation and Analysis Center (NISAC), and the National Communication System (NCS). *See* § 201, 116 Stat. at 2148-49.

Substantively, the DHS Act granted legal protections, such as Freedom of Information Act (FOIA) exemptions, to non-federal entities that voluntarily provided information to the DHS.[50]

The Homeland Security Act also called for the initiation of a critical infrastructure protection program.[51] Accordingly, in February 2003, the White House released its National Strategy to Secure Cyberspace (NSSC).[52] The NSSC acknowledged the importance of protecting the nation's CIs, but nonetheless made it clear that the federal government was not, nor would it be, responsible for securing private computer networks.[53]

Following the release of the NSSC, the White House issued Homeland Security Presidential Directive 7 (HSPD-7)—Critical Infrastructure Identification, Prioritization and Protection on December 17, 2003.[54] Inter alia,[55] HSPD-7 established the Critical Infrastructure

---

50. The Homeland Security Act provides protection to critical infrastructure information that is "voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose . . . ." § 214(a)(1), 116 Stat. at 2152. These non-federal entities are exempt from disclosure. Specifically, under the Freedom of Information Act these entities "shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official" and are exempt from requirements of the Federal Advisory Committee Act. *Id.* § 214(a)(1)(B), (b), 116 Stat. at 2152-53. For an analysis of critical infrastructure protection in light of the Freedom of Information Act, see Cara Muroff, Note, *Terrorists and Tennis Courts: How Legal Interpretations of the Freedom of Information Act and New Laws Enacted to Prevent Terrorist Attacks Will Shape the Public's Ability to Access Critical Infrastructure Information*, 16 U. FLA. J.L. & PUB. POL'Y 149 (2005); Kristen Elizabeth Uhl, Comment, *The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security*, 53 AM. U.L. REV. 261 (2003).

51. § 213, 116 Stat. at 2152 (codified at 6 U.S.C. § 132 (2012)).

52. EXEC. OFFICE OF THE PRESIDENT, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf [https://perma.cc/4A2W-5QH8]; Jensen, *supra* note 26, at 1558.

53. EXEC. OFFICE OF THE PRESIDENT, *supra* note 52, at 11 ("The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector.").

54. Homeland Security Presidential Directive/HSPD-7—Critical Infrastructure Identification, Prioritization, and Protection, 2 PUB. PAPERS 1739 (Dec. 17, 2003) [hereinafter HSPD-7].

55. HSPD-7 stated, "It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could: (a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction; (b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety; (c) undermine State and local government capacities to maintain order and to deliver minimum essential public services; (d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services; (e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or (f) undermine the public's morale and confidence in our national economic and political institutions." *Id.* at 1740.

Protection Policy Coordinating Committee, which was tasked with advising the Homeland Security Council on infrastructure security[56] and assigned critical infrastructure tasks to federal departments and agencies, some of which were classified as Sector Specific Agencies (SSAs) and made responsible for the protection of CIs.[57] Each SSA contributed to the newly developed National Infrastructure Protection Plan (NIPP) under the auspices of the Secretary of Homeland Security. The first NIPP was released in 2006,[58] and has been updated twice since: in 2009 and 2013.[59] The 2006 NIPP listed twelve CIs as assets of national importance[60] and five categories of key assets.[61]

In 2006, consistent with Section 201 of the Homeland Security Act, the DHS formed a Critical Infrastructure Partnership Advisory Council (CIPAC) "to facilitate interaction between governmental entities and representatives from the community of critical infrastructure

56. MOTEFF, *supra* note 12, at 10-11.

57. Specifically, the Department of Agriculture was in charge of "agriculture, food (meat, poultry, egg products);" Health and Human Services was in charge of "public health, healthcare, and food (other than meat, poultry, egg products);" the Environmental Protection Agency was in charge of "drinking water and water treatment systems;" the Department of Energy was in charge of "energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities;" the Department of the Treasury was in charge of "banking and finance;" the Department of the Interior was in charge of "national monuments and icons;" and the Department of Defense was in charge of "defense industrial base." HSPD-7, *supra* note 54, at 1741. Each SSA is required to "(a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; (b) conduct or facilitate vulnerability assessments of the sector; and (c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources." *Id.*

58. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN (2006), https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf [https://perma.cc/PMW2-KU6F].

59. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO ENHANCE PROTECTION AND RESILIENCY (2009), https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf [https://perma.cc/MZ7U-7JH7]; DEP'T OF HOMELAND SEC., NIPP 2013: PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013), https://www.dhs gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf [https://perma.cc/2HFY-FUD9] [hereinafter 2013 NIPP].

60. The twelve identified critical infrastructure sectors in the United States by the 2006 NIPP: (1) defense industrial base; (2) food and agriculture; (3) public health and health care; (4) emergency services; (5) energy; (6) transportation systems; (7) banking and finance; (8) information technology; (9) telecommunications; (10) drinking water and water systems; (11) chemicals; and (12) postal and shipping. *See* DEP'T OF HOMELAND SEC., *supra* note 58, at 3.

61. (1) National monuments and icons; (2) nuclear reactors, materials, and waste; (3) dams; (4) government facilities; and (5) commercial facilities. *See id.*

owners and operators."[62] Since then, DHS has continued to fund various centers and offices, each charged with analyzing CI protection plans and measures.[63]

The Obama Administration—Data Sharing and (Very) Gentle Nudging: The Obama Administration ordered a reexamination of the U.S. CI protection strategy,[64] which led to the publication of two policy papers: the Cyberspace Policy Review in 2009[65] and the International Strategy for Cyberspace in 2011.[66] The reports again emphasized the importance of protecting CIs; in response, the Obama Administration formed the U.S. Cyber Command (CYBERCOM) to centralize U.S. cyber operations and secure dot-mil domains.[67] Neither publication brought substantial changes to the overall strategy noted thus far.

The Obama Administration released Presidential Policy Directive 21 (PPD-21) in February 2013, *Critical Infrastructure Security and Resilience*, which superseded HSPD-7.[68] PPD-21 called for strengthening CI security and resilience by refining and clarifying the organizational relationships across the federal government, enabling effective information exchange (including real time data sharing), and implementing integration and analysis capabilities to inform planning and

---

62. *Critical Infrastructure Partnership Advisory Council*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/critical-infrastructure-partnership-advisory-council [https://perma.cc/M9U7-JX5Q]; Homeland Security Act of 2002, Pub. L. No. 107-296, § 201, 116 Stat. 2135, 2145-49 (codified at 6 U.S.C. § 121 (2012)).

63. For example: Homeland Infrastructure Threat and Risk Analysis Center (HITRAC); National Infrastructure Simulation and Analysis Center (NISAC); and Office of Cyber & Infrastructure Analysis (OCIA). *See, e.g.*, *Office of Cyber and Infrastructure Analysis (OCIA)*, DEP'T OF HOMELAND SEC. (Jan. 11, 2017), https://www.dhs.gov/office-cyber-infrastructure-analysis [https://perma.cc/B7BJ-U8NT].

64. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-432T, NATIONAL CYBERSECURITY STRATEGY: KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE 1, 4 (2009), http://www.gao.gov/new.items/d09432t.pdf [https://perma.cc/C39Z-EKC3]; Scott J. Shackelford & Andraz Kastelic, Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity 14 (Jan. 5, 2015) (unpublished manuscript), http://works.bepress.com/scott_shackelford/13 [https://perma.cc/7PZ6-VGU7].

65. EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [https://perma.cc/8NLU-82NX].

66. EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [https://perma.cc/A6CQ-ZNT2].

67. Shackelford & Kastelic, *supra* note 64, at 14; *U.S. Cyber Command (USCYBERCOM)*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ [https://perma.cc/BG8E-APJH].

68. MOTEFF, *supra* note 12, at 11; Press Release, Office of the Press Sec'y, White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/DWF6-4K9P].

operational decisions regarding CIs.[69] In addition to expanding public-private information sharing, PPD-21 listed and identified sixteen CI sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.[70] Each sector is linked up with an SSA as the lead coordinator. NIPP 2013 was released shortly thereafter and updated the previous NIPP.[71]

Roughly around the same time, President Obama signed Executive Order 13,636, Improving Critical Infrastructure Cybersecurity,[72] which was designed to develop, promote, and incentivize a voluntary cybersecurity framework and collaboratively develop and implement risk-based approaches to cybersecurity to protect privacy and civil liberties.[73] Additional steps were also taken to promote voluntary CI frameworks. In February 2014, the National Institute of Standards and Technology (NIST) published a voluntary cybersecurity framework for all CI operators: *Framework for Improving Critical Infrastructure Cybersecurity*.[74] It contains standards, guidelines, and practices to encourage CI protection, mainly through public-private partnerships.

---

69. Press Release, Office of the Press Sec'y, *supra* note 68.

70. *Id.*

71. More specifically, the 2013 NIPP "[e]levates security and resilience as the primary aim of critical infrastructure homeland security planning efforts; [u]pdates the critical infrastructure risk management framework and addresses alignment to the National Preparedness System, across the prevention, protection, mitigation, response, and recovery mission areas; [f]ocuses on establishing a process to set critical infrastructure national priorities determined jointly by the public and private sector; [i]ntegrates cyber and physical security and resilience efforts into an enterprise approach to risk management; [a]ffirms that critical infrastructure security and resilience efforts require international collaboration; [s]upports execution of the *National Plan* and achievement of the National Preparedness Goal at both the national and community levels, with focus on leveraging regional collaborative efforts; and [p]resents a detailed Call to Action with steps that will be undertaken, shaped by each sector's priorities and in collaboration with critical infrastructure partners, to make progress toward security and resilience." 2013 NIPP, *supra* note 59, at 4.

72. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

73. *Id.*

74. More specifically, NIST focuses on risk management processes as a best practice for CIP. The proposed framework consists of three ties: framework core, framework profile, and framework implementation. *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 4-5 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/JV28-3KBL].

Shortly thereafter, Congress enacted the Cybersecurity Enhancement Act[75] and expanded the NIST's responsibilities to include supporting the development of voluntary, industry-led standards and practices to reduce CI cyber risks.[76] The Act also vested the Office of Science and Technology Policy with developing federal cybersecurity research and development plans. While the private sector was not subject to mandatory requirements, these instruments clearly signal the government's expectations of the private sector.

Information sharing initiatives continued to unfold. In December 2014, Congress passed the National Cybersecurity Protection Act (NCPA),[77] which formed the National Cybersecurity and Communications Integration Center (NCCIC). This center is tasked with creating a platform for voluntary government and private sector information sharing regarding cybersecurity threats, incident response, and technical assistance. Subject to DHS discretion, this center could include representatives from federal agencies, state and local governments, and private sector CI owners and operators.[78]

In addition, President Obama issued Executive Order 13,691 on cybersecurity information in February 2015.[79] This order builds upon Executive Order 13,636 and PPD–21, and "strongly encourage[s] the . . . formation of Information Sharing and Analysis Organizations (ISAOs)."[80] NCCIC and ISAOs are to collaborate on information sharing related to cybersecurity risks and threats, incident response, and strengthening information security systems.[81] Executive Order 13,691 determines that that information sharing must be conducted while simultaneously protecting the privacy and civil liberties of individuals, preserving business confidentiality, and protecting the shared information, among other things.[82]

In December 2015, President Obama signed the Consolidated Appropriations Act, which included a provision titled the "Cybersecurity Act of 2015."[83] The first chapter of the Cybersecurity Act is largely based on a highly controversial bill, the Cyber Information Sharing

75. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971.

76. § 101(b), 128 Stat. at 2972-73.

77. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066.

78. CONGRESS PASSES FOUR CYBERSECURITY BILLS, NAT'L L. REV. (Dec. 13, 2014), http://www.natlawreview.com/article/congress-passes-four-cybersecurity-bills [https://perma.cc/ZQR2-HMCA].

79. Exec. Order No. 13,691, 80 Fed. Reg. 9349 (Feb. 20, 2015).

80. *Id.* at 9349.

81. *Id.*

82. *Id.*

83. *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, 2244.

Act (CISA), which attracted substantial attention.[84] For security purposes, the Cybersecurity Act authorizes private entities to monitor their information systems, initiate defensive measures, and share cyber threat indicators or defensive measures with other private sector entities and the government.[85] The Act places some restrictions on information sharing to protect privacy interests,[86] and mainly forms a framework for the voluntary sharing of cyber threats, with the DHS acting as a central hub. Accordingly, CI operators and other private sector entities can legally share a "cyber threat indicator"[87] for a "cybersecurity purpose."[88] In exchange, they are granted immunity from liability, provided antitrust protections, and are exempt from any related requests under FOIA.[89] While the final version of this Act was controversial,[90] it notably did not expand DHS's authority to include regulation of CIs as proposed under the original CISA Bill.[91] Under the Cybersecurity Act, the DHS ultimately functions as a mere infor-

---

84. *See* Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015). For criticism on previous versions of CISA, see, e.g., Eldar Haber, *The Cybersecurity Information Sharing Act (CISA)*, CYBER FORUM (Aug. 7, 2015, 7:27 PM), http://web-law.haifa.ac.il/he/Research/ResearchCenters/cyberforum/cyberblog/Lists/Posts/Post.aspx?ID=20 [https://perma.cc/A2MX-H6GX]; Sam Thielman, *Controversial Cybersecurity Bill on Hold as Experts Charge It Won't Stop Hackers*, GUARDIAN (Aug. 5, 2015), http://www.theguardian.com/world/2015/aug/05/cybersecurity-cisa-bill-hackers-privacy-surveillance [https://perma.cc/32BQ-7JUD].

85. *See* § 104, 129 Stat. at 2940-41.

86. For example, prior to information sharing, the network operator must remove "any information not directly related to a cybersecurity threat" that the operator "knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual." *Id.* § 104(d)(2)(A), 129 Stat. at 2942.

87. The term "cyber threat indicator" is defined as "information that is necessary to describe or identify" any of the following items or any combination of them:

> [M]alicious reconnaissance . . . ; a method of defeating a security control or exploitation of a security vulnerability; a security vulnerability . . . ; a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; the actual or potential harm caused by an incident . . . ; [or] any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law.

See id. § 102(6)(A)-(G), 129 Stat. at 2937.

88. *Id.* § 102(4), 129 Stat. at 2936.

89. *Id.* § 106(b), 129 Stat. at 2951 (liability immunity); *id.* § 104(e), 129 Stat. at 2943 (antitrust protections); *id.* § 104(d)(4)(B)(ii), 129 Stat. at 2942-43 (FOIA exemption).

90. *See, e.g.*, Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, WASH. POST (Dec. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws [https://perma.cc/TV46-R7ZQ]. There are also bills calling for the repeal of the Cybersecurity Act of 2015. *See, e.g.*, H.R. 4350, 114th Cong. (2016).

91. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 407 (2015).

mation hub. It is also tasked with publishing (1) guidelines for reporting cyber threats; (2) procedures that governmental agencies must follow for handling data received through this mechanism; and (3) a set of interim privacy and civil liberties guidelines governing the receipt, retention, use, and dissemination of data by federal entities.[92] The Act does not constitute a substantial change in U.S. CI policy as it has unfolded in recent decades. There are currently several proposed bills that relate to Critical Infrastructure Protection (CIP) and could expand the framework for information sharing between CI operators and the government.[93]

2. The Exception—Direct Governmental Intervention

In general, the United States supports voluntary participation in CI protection policies. There are, however, two notable and substantial exceptions: U.S. chemical and energy sectors are subject to various forms of aggressive regulation, including mandatory government-set standards.[94] Understanding these exceptions is of great importance, as either their universal or selective expansion is something to be considered.

In 2007, Congress enacted CI regulation within a specific sector: high-risk chemical facilities. Under the Homeland Security Appropriations Act, Congress mandated the establishment of "risk-based performance standards for security of chemical facilities," the development of vulnerability assessments, and "implementation of site security plans for chemical facilities."[95] Note that even this regulatory scheme does not call for promulgation of specific rules; instead, it requires general and broad standards to be determined by the DHS. A

92. *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, § 105, 129 Stat. 2242, 2943-50.

93. *See, e.g.*, Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2012). The Protecting Cyber Networks Act—approved by the U.S. House of Representatives—sets a framework for private companies to provide information on any suspicious activity on their networks in exchange to immunity from consumer lawsuits. *See* Protecting Cyber Networks Act, H.R. 1560, 114th Cong. § 203 (2015). Under the Act, the NCCIC serves as "the lead federal civilian interface for multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, and cybersecurity risks for federal and non-federal entities." *H.R.1560—Protecting Cyber Networks Act*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/1560 [https://perma.cc/24WV-7796].

94. Notably, CI operators that facilitate in U.S. ports are subject to the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064, which "requires facilities at ports, and certain vessels, to conduct vulnerability assessments and to develop and implement security plans . . . ." MOTEFF, *supra* note 12, at 30.

95. Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388.

2014 amendment to this Act granted the federal government additional regulatory measures, including those related to its enforcement via civil penalties and orders to cease operations when needed.[96]

Since 2007, the energy sector has also been subject to mandatory requirements pertaining to cyber protection for its CI operators. Authorized by the Energy Policy Act, the Federal Energy Regulatory Commission (FERC)[97] certified the North American Electric Reliability Corporation (NERC)—which is *not* a governmental entity—as an Electric Reliability Organization (ERO). NERC was tasked with developing, auditing for compliance, and enforcing mandatory reliability standards for bulk power systems, subject to FERC approval.[98] Since its mandate, FERC has approved four CIP Reliability Standards.[99]

The noted regulatory dynamic, which involves both public and private parties, constitutes an interesting form of co-regulation that has been subject to ongoing criticism in various forms. For one, commentators argue that the FERC (the government entity) is unable to carry out its duties properly.[100] Others claim that the results of the FERC's approval process highly favor industry objectives.[101] An additional critique set forth by the FERC itself notes that the process is excessively transparent (thus providing adversaries with extensive information

---

96. *See* Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, Pub. L. No. 113-254, § 2104, 128 Stat. 2898, 2912-13.

97. Since 2005, the FREC regulates "over 1,500 organizations, including municipal utilities, Federal power administrations, electric cooperatives, and even the Tennessee Valley Authority and the U.S. Army Corps of Engineers." Susan J. Court, *Federal Cyber-Security Law and Policy: The Role of the Federal Energy Regulatory Commission*, 41 N. KY. L. REV. 437, 438 (2014); FED. ENERGY REGULATORY COMM'N, FACT SHEET: ENERGY POLICY ACT OF 2005 (2006), https://www.ferc.gov/legal/fed-sta/epact-fact-sheet.pdf [https://perma.cc/P363-SRUY].

98. *See, e.g.*, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706-C, 127 FERC ¶ 61,273 (June 18, 2009); Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706-B, 126 FERC ¶ 61,229 (Mar. 19, 2009); Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706-A, 123 FERC ¶ 61,174 (May 16, 2008); Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706, 122 FERC ¶ 61,040 (Jan. 18, 2008); Dan Assaf, *Models of Critical Information Infrastructure Protection*, 1 INT'L J. CRITICAL INFRASTRUCTURE PROTECTION 6, 7-8 (2008).

99. *See* Ryan Ellis, *Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?*, 12 IEEE SECURITY & PRIVACY 48, 48 (2014); Version 5 Critical Infrastructure Protection Reliability Standards, Order No. 791, 145 FERC ¶ 61,160 (Nov. 22, 2013). Indeed, there were actually five plans suggested, but one was never approved. *See* Court, *supra* note 97, at 443-44.

100. Court, *supra* note 97, at 454 (discussing the FERC's difficulty in responding to cyber risks in a timely manner).

101. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-117, ELECTRICITY GRID MODERNIZATION: PROGRESS BEING MADE ON CYBERSECURITY GUIDELINES, BUT KEY CHALLENGES REMAIN TO BE ADDRESSED 22-26 (2011), http://www.gao.gov/assets/320/314410.pdf [https://perma.cc/BYJ4-LH9K] (listing key challenges the electricity industry faces); *see also* Palmer, *supra* note 17, at 340-41.

regarding vulnerabilities) and rigid, both factors that undermine its effectiveness. In response to critiques, the FERC argues the solution is to expand its authority.[102] On the other hand, at least one commentator[103] noted that even after acknowledging this regulatory scheme's shortcomings, it might prove to be an optimal solution to regulate CI cyber threats. The scheme might be slow, but it allows for a bottom-up process that incorporates the knowledge accumulated by the industry.[104]

Nuclear power plants are another energy sector that has also been closely regulated. The operation of such plants must meet specific standards of competence and activity that include, inter alia, the assessment of their vulnerabilities to a variety of attacks and mandate the necessary actions to address their vulnerabilities. The Nuclear Regulatory Commission (NRC) is responsible for the regulation and enforcement of this industry.[105] To do so, the NRC published a detailed 'Regulatory Guide' to help firms meet the required standards.[106] However, the plants' adherence to the noted guide is voluntary and security measures can be met through alternative means.

This summary of the U.S. approach to CI cyber risk protection indicates that the American strategy mostly relies on presidential directives, executive orders, legislation, guidelines, and agency policies in specific sectors. Furthermore, with several noted sector-specific exceptions, the U.S. approach mostly facilitates public-private information sharing and depends upon market forces. However, a final caveat is due. Even though the government does not mandate specific standards, the benefits of the implementation and enforcement of these standards cannot be easily ignored—for example, voluntary implementation of government-set guidelines could shield private CIs from governmental and public scrutiny and help rebut negligence claims in tort lawsuits, all which might render these standards effectively mandatory.[107] Since this final assertion has yet to be tested in a court of law, at best it remains speculative.

---

102. Court, *supra* note 97, at 454-55.

103. Ellis, *supra* note 99, at 52-54.

104. *Id.*

105. *See* DEP'T OF HOMELAND SEC., NUCLEAR REACTORS, MATERIALS, AND WASTE SECTOR-SPECIFIC PLAN: AN ANNEX TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN 2 (2010), http://www.dhs.gov/xlibrary/assets/nipp-ssp-nuclear-2010.pdf [https://perma.cc/G894-YCTC]; MOTEFF, *supra* note 12, at 30.

106. U.S. NUCLEAR REGULATORY COMM'N, REGULATORY GUIDE 5.71: CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES (2010), https://scp.nrc.gov/slo/regguide571.pdf [https://perma.cc/6AVJ-J4LY].

107. According to Stewart Baker: "In the real world, these 'voluntary' standards will be quasi-mandatory, because companies that don't meet them could face lawsuits after suffering a breach. They will also provide some liability protection for industry, since under tort law, following government standards is a good way to rebut claims of negligence." *See* Mark

B. Regulating Cyber-Risks of CI—A Comparative View

While the United States seems to be set (for the time being) on a specific regulatory trajectory, other nations facing very similar challenges have chosen a different approach, and still others are contemplating changing their traditional paths.

CI regulation in the European Union has been addressed both at the state and the union level. As was the case in the United States, external events acted as the regulatory trigger, most notably the Madrid train bombings of 2004.[108] Here too, the early response was in the form of institution building. The European Council first required the European Commission to prepare an overall program to protect European CIs.[109] In addition, in that same year, the European Network and Information Security Agency (ENISA) was established to prevent, address, and respond to network and information security problems and advise member states on these matters.[110] ENISA will prove to be a key player in the promotion of data sharing between CIs and governments as well as among CIs themselves.

The next step in EU regulation was far more concrete and included specific recommendations and directives. At first, in 2006, the Commission proposed a CIP Directive, which, among other things, embraced the European Programme for Critical Infrastructure Protection (EPCIP).[111] The directive was approved in 2008[112] and mandated that EU members enact domestic legislation incorporating EPCIP standards. While the Directive marked an important step in EU CIP, it had a limited scope.

Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR (Feb. 13, 2013), http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts [https://perma.cc/Q3JR-6GV8]; *see also* John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOT POINT SEC.: INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework [https://perma.cc/QN98-MWGX].

108. *See March 11, 2004: Terrorists Bomb Trains in Madrid*, HISTORY, http://www.history.com/this-day-in-history/terrorists-bomb-trains-in-madrid [https://perma.cc/P2EA-8QB3].

109. *See* Asa Fritzon et al., *Protecting Europe's Critical Infrastructures: Problems and Prospects*, 15 J. CONTINGENCIES & CRISIS MGMT. 30, 32 (2007). A 'Green Paper' on these issues was also published in 2005. *See Commission Green Paper on a European Programme for Critical Infrastructure Protection*, at 2, COM (2005) 576 final (Nov. 17, 2005), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN [https://perma.cc/44MF-NCDZ].

110. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency 2004 O.J. (L 77) 1, 2.

111. *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, COM (2006) 786 final (Dec. 12, 2006).

112. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, 2008 O.J. (L 345) 75, 75.

First, it only regulated two sectors: energy and transportation. In addition, as it only focused on EU infrastructures, it only applied to those infrastructures shared by at least two EU member states. In general, the Directive faced wide criticism, particularly in light of its failure to impose obligations on CI operators beyond reporting attacks.[113]

EU actions to this point did not address specific cyber challenges. Yet this was bound to change, and on March 30, 2009, the EU Commission adopted the Critical Information Infrastructure Protection Communication.[114] Among other things, this communication addressed the need to establish criteria for European CI protection in the field of Information and Communication Technologies (ICTs).[115] In March 2011, the Commission continued its efforts to enhance CIP and called for the creation of an EU coherent and cooperative approach that incorporated a global coordination strategy.[116] Here again, the Commission emphasized the importance of ICT resilience, and on June 12, 2012, the EU Parliament adopted a new CIP resolution that focused on ICT.[117] This resolution proposed, inter alia, forming public and private stakeholders partnerships at the union level and encouraged them to develop and implement security standards to increase civilian national and European critical information infrastructure resilience. Therefore, the EU experience has thus far been quite similar to that of the United States—its regulations mostly focused on facilitating data sharing, promoting voluntary standards developed by public-private partnerships, and carving out sector-specific exceptions.

However, substantial changes in EU policy are on their way. In 2016, the European Parliament adopted a new directive for CI cyber

---

113. For criticism on the Directive, see *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)*, at 12, SWD (2012) 190 final (June 22, 2012).

114. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, "Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience,"* COM (2009) 149 final (Mar. 30, 2009).

115. *Policy on Critical Information Infrastructure Protection (CIIP)*, EUROPEAN COMM'N (July 2, 2013), https://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip [https://perma.cc/AH5J-JP2W].

116. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, "Achievements and next Steps: Towards Global Cyber-security,"* COM (2011) 163 final (Mar. 31, 2011).

117. European Parliament Resolution on Critical Information Infrastructure Protection—Achievements and Next Steps: Towards Global Cyber-security (2011/2284(INI)), P7_TA(2012)0237, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167.

security.[118] The directive "*concerning measures to ensure a high common level of network and information security across the Union*,"[119] or the NIS Directive, includes several distinct steps. First, it moves to actively promote data sharing. For instance, the directive mandates that member states establish competent Network Information Security (NIS) authorities to facilitate data sharing and cooperation, as well as Computer Emergency Response Teams (CERTs). Next, it requires states to plan and consider their responses to attacks on CIs by adopting national NIS strategies and NIS cooperation plans. And the directive extends beyond the confines of the current U.S. regulatory strategy; under Article 14, it mandates that CI operators (addressed and defined as "essential services") generate a cyber risk assessment and apply appropriate and proportionate measures to ensure information security. Even privately held CIs are required to report security incidents to the government, and noncompliance will result in sanctions.[120] A separate, more lenient regime was set in place in Article 16 for "digital service providers," which were defined to include search engines, cloud computing services, and online marketplaces.[121]

The European Union has an aggressive stance on creating a specific sector strategy for communication services. A 2009 amendment to the EU communication directive requires member states enact legislation regulating public communication networks, even if they are at times private entities.[122] Accordingly, communication companies must take appropriate technical and organizational measures to manage security risks to their networks and services.[123] The directive further mandates that member states promulgate legislation, requiring these firms to submit a security audit to a national authority and to permit mandatory inspection of their sites to ensure that appropriate measures were implemented.

---

118. *European Comm'n—Fact Sheet: Directive on Security of Network and Information Systems* (July 6, 2016), http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm [https://perma.cc/LF7M-ZZY4].

119. *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, COM (2013) 48 final (Feb. 7, 2013).

120. Simon Shooter & Toby Bond, *European Cybersecurity Directive Moves Closer to Becoming a Reality*, BIRD & BIRD (Feb. 17, 2014), http://www.twobirds.com/en/news/articles/2014/global/european-cybersecurity-directive-moves-closer-to-becoming-a-reality [https://perma.cc/LK6Y-C9D5]; *European Comm'n—Fact Sheet*, *supra* note 118.

121. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 1, 3-4, 13, 21-22.

122. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 O.J. (L 337) 37, 54.

123. *Id.* arts. 13a, 13b, at 54-55.

Beyond EU regulation, EU Member States have deployed independent and diverse measures to protect CIs from cyber attacks.[124] Some chose a more lenient approach, others a far stricter one. For instance, in the UK,[125] CI operators can choose whether to receive advice from a governmental authority, the National Cyber Security Centre (NCSC),[126] which is similar to the voluntary scheme applied in the United States. Other EU states enacted regulatory schemes that include government oversight. For instance, the Czech Republic recently passed cybersecurity legislation that specifies CIP operator requirements.[127] Furthermore, the Czech National Security Authority was empowered with discretionary authority to take reactive measures to resolve cybersecurity incidents or to secure information systems and networks.[128] Germany had generally implemented voluntary infrastructure protection measures with few legal requirements. Yet recently this changed when Germany created a CIP Implementation Plan, termed "KRITIS," with the declared goal of encouraging public-private information sharing and cooperation.[129] Furthermore, even more recently, Germany chose a stricter approach by passing a new law *requiring* CI operators introduce cybersecurity measures or face fines of up to € 100,000 (in addition to strict reporting requirements of cyber attacks).[130] The new Czech and German strategies seem to

---

124. For further information, see a report by the EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC., METHODOLOGIES FOR THE IDENTIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE ASSETS AND SERVICES 9-12 (2014), https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport [https://perma.cc/95Q8-2AY7]; *see also* Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 153-57 (2014) (summarizing the evolution of EU cybersecurity policymaking).

125. We acknowledge that the UK might be leaving the European Union in the next couple of years. The text refers to the period during which it was an EU member.

126. *See About Us*, NAT'L CYBER SEC. CTR., https://www.ncsc.gov.uk/about-us [https://perma.cc/2WWR-E96E] (last visited Mar. 23, 2018).

127. Act No. 181 on Cyber Security and Change of Related Acts (Act on Cybersecurity), § 4(3) (Czech Republic).

128. *Id.* § 13.

129. FED. REPUBLIC OF GER., FED. MINISTRY OF THE INTERIOR, NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION (CIP STRATEGY) 14-17 (2009), http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile [https://perma.cc/7RWC-J49D]; FED. REPUBLIC OF GER., FED. MINISTRY OF THE INTERIOR, CYBER SECURITY STRATEGY FOR GERMANY 5 (2011), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile [https://perma.cc/4Q5N-GEMQ].

130. zur Erhöhung der Sicherheit informationstechnischer Systeme [IT-Sicherheitsgesetz] [Increasing the Security of Information Technology Systems] [IT Security Law], July 17, 2015, BUNDESGESETZBLATT, Teil I [BGBL I] at 1324 2015 I (Ger.), https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27175315%27%5D&skin=pdf&tlevel=-2&nohist=1 [https://perma.cc/BEZ9-UXKW]; *see also* Detlev Gabel & Marc Schuba, *Germany Rolls*

acknowledge the novel cyber risks to CI stability and chose to respond to these risks by enhancing government regulatory reach.

Other countries have already established such an elaborate regulatory scheme. A case in point, consider Israel's regulatory scheme. Clearly, Israel faces a multitude of threats both in the physical and cyber worlds. It is therefore no surprise that it has closely regulated CI cyber security[131] and chosen a strict and unique government approach to protecting CIs. The Israeli Security Law (2002 amendment) established the National Information Security Authority (NISA) (a unit within the General Security Service).[132] NISA was "charged with [the] professional guidance of the institutions under its responsibility in the area of protecting critical computer infrastructures."[133] The Israeli legislation also features a list of CIs that are subject to NISA authority.[134] Inclusion in the CI list is not sectorial; rather it is an ad hoc list of specific bodies that are subject to the regulatory scheme.

The official role of the NISA[135] is to guide, oversee implementation, and sanction for noncompliance.[136] All CI-defined companies must appoint a chief security officer, who is responsible for essential computer system security, subject to NISA approval and guidelines. NISA is also empowered to direct and instruct the chief security officer on required security actions (including reporting) and, most importantly, to inspect the regulated entity. Very recent changes in Israeli law are shifting

---

Out IT Security Act, WHITE & CASE TECH. NEWSFLASH (Aug. 18, 2015) (discussing German IT Security Act), http://www.whitecase.com/publications/article/germany-rolls-out-it-security-act# [https://perma.cc/EGV8-73BF]; *Germany Passes Strict Cyber-security Law to Protect 'Critical Infrastructure'*, RT NEWS (July 11, 2015), http://www.rt.com/news/273058-german-cyber-security-law/? [https://perma.cc/AD4F-MX8D].

131. *See, e.g.*, SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 188 (2014) ("Geopolitical concerns and several wars have put Israel at the forefront of cybersecurity, with tools reportedly rivaling U.S. capabilities.").

132. *See* National Security Ministerial Committee Resolution No. 84/B of December 11, 2002 (Isr.); Regulation of Security in Public Bodies Law of 1998, 5758-1998, SH No. 1685 p. 348, as amended (Isr.).

133. Lior Tabansky, *Critical Infrastructure Protection against Cyber Threats*, 3 MIL. & STRATEGIC AFF. 61, 77 n.18 (2011) (quoting the responsibilities of NISA as previously appeared on the website of the General Security Service).

134. *See supra* note 132.

135. The Israeli government is currently leading an effort to transfer most of NISA responsibilities to the newly formed Cyber Bureau. *See* Advancing National Cyberspace Capabilities, Isr. Res. No. 3611 (Aug. 7, 2011), http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf [https://perma.cc/9Q4B-J5NB]; *see also* Daniel Benoliel, *Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study*, 16 N.C. J.L. & TECH. 435, 445 (2015) (exploring the tasks of the Israeli National Cyber Bureau).

136. Tabansky, *supra* note 133, at 72 (describing the Israeli CIP model).

some of these responsibilities and authorities to a newly-minted Cyber Authority, which is part of the Prime Minister's Office.[137]

To conclude this brief comparative study, the European Union's approach to cyber CIP is relatively non-intrusive. The European Union acknowledges the importance of a national CIP agency; information sharing between member states; and forming mandatory advisory and oversight frameworks. However, this approach is relatively moderate (in comparison, for instance, to Israel's). Perhaps future developments, such as those currently under discussion in the European Union and specific member states, will change current CIP strategies. Several EU states have already taken steps in this direction.

IV. MODELS OF CYBER CIP: MARKET-BASED & EX POST REGULATION

As our comparative analysis demonstrates, the current U.S. CI cyber risk regulatory strategy is premised on voluntary participation. Yet this strategy should at least be revisited (if not revised) given both the transitions in the risk profile of cyber events and regulatory changes being considered in other countries. Optimal regulatory schemes must carefully balance costs, benefits, and challenges of various regulatory models. This Part seeks out such an optimal scheme, and commences the discussion in Section A by first examining a regulatory regime that features the most minimal level of regulation and is almost solely governed by market forces. To some extent, this is the current U.S. regime. Section A then proceeds to identify this regime's systematic failures and shortcomings. Thereafter, in Sections B and C this discussion moves to analyze more demanding regulatory schemes, which feature enhanced information sharing and ex post liability for damages caused by security failures, all the while accounting for the specific context of cyber CIs.

A. The Market-Based Approach

To establish whether CIP necessitates regulatory intervention, we must determine whether social and market forces are able to generate an equilibrium according to which firms provide adequate CIP on their own initiative and with their own resources. Private CI entities have substantial incentives to provide high levels of protection and they indeed invest in measures to protect their firm's assets (both physical and virtual), its reputation and share price, and its customers from harm. This is because interrupted and discontinued services would

137. Law for the Regulation of Security in Public Bodies, 5758-1998, SH No. 1739 §§ 2a, 10 (Isr.); *see also* Assaf, *supra* note 98, at 8-9.

likely increase consumer dissatisfaction, leading to reduced consumption or even termination of the contract.[138] If this is the case, limited or no government regulation could prove to be the optimal strategy. According to this line of thought, regulatory intervention is needed only when *market failures* are identified and prevent the market from reaching an acceptable equilibrium point. Market failures are the instance at which CIs require external intervention to assure a suitable level of protection.

The 'market will solve it' argument might seem to be an analytical 'straw man,' especially when pertaining to the market for public utilities, which are often regulated closely and feature multiple systematic failures. Yet this argument cannot be easily rejected for at least two reasons. First, to a great extent this argument constitutes the self-proclaimed regulatory strategy in the United States today and, therefore, must be given some additional thought.[139] Second, even though the outcome of this limited regulatory scheme is problem-ridden, it still features notable benefits. It reduces regulatory costs associated with both norm-setting and complex enforcement, which could prove substantial in this hi-tech context. It limits fears and problems associated with regulatory capture and could also reduce potential systematic errors found in governmental regulation. Arguably, private CI operators are in a better position than the government to determine which security measures are required to protect their own infrastructures, especially concerning technological matters.[140] Beyond economic benefits, limited governmental regulation generates social value. Lack of governmental involvement decreases, and in some instances, eliminates, constitutional and human rights violations, especially those pertaining to the right to privacy. Government meddling with security levels and alerts could quickly evolve into government data collection—a practice that generates substantial concerns.

Yet the claim that market and social forces alone are sufficient to ward off cyber risks to CIs faces very substantial challenges, because

---

138. For similar arguments by industry representatives, see PAUL ROSENZWEIG, CYBER WARFARE: HOW CONFLICTS IN CYBERSPACE ARE CHALLENGING AMERICA AND CHANGING THE WORLD 100-01 (2013); THERESE KERFOOT, CYBERSECURITY: TOWARDS A STRATEGY FOR SECURING CRITICAL INFRASTRUCTURE FROM CYBERATTACKS 6 (2012), http://siliconflatirons.org/documents/publications/report/CybersecurityPaper.pdf [https://perma.cc/E39V-6EFL].

139. It seems like the market-based approach currently leads CIP regulation in the United States. *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 120-22 (2010).

140. *See, e.g.*, Palmer, *supra* note 17, at 297-98 ("[T]hose who oppose government mandates, particularly those in the critical infrastructure industry, believe the government 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.").

the market and social forces CIs are subjected to generate insufficient incentives for CI owners and thus will not lead to optimal outcomes in this context.[141] These challenges most likely will lead to insufficient investments in cyber protection[142] and sub-optimal responses to unfolding cyber threats. These outcomes result from three distinct causes that we now discuss separately: (1) Market failures and other barriers undermine CI customers' abilities to signal their discontent with insufficient levels of cyber protection, and therefore, the noted equilibrium will not be reached; (2) inadequate cyber-protection generates negative externalities. Market forces alone do not provide CI operators with sufficient incentives to internalize the costs and risks they might cause; and (3) CI operators lack inherent information and knowledge, which impedes their ability to provide a sufficient level of protection. Recognizing that each concern is distinct is crucial because, as set out below, each one requires a different response and relies on a separate set of facts and assumptions.

(1) **Market Failures/Signaling Problems**: In theory, firms respond to consumer discontent (or the fear of them being discontent enough to leave) and take action. Yet this dynamic will not unfold if consumers lack the ability or opportunity to indicate their discontent—for instance, when a firm is a monopoly or operates in an oligopolistic market. Additionally, in many instances markets feature high switching costs;[143] that is, the high costs of changing service providers limit the consumers' signaling abilities. Finally, the fear of a drop in stock prices due to security breaches does not appear to be substantial given mixed results found in the personal data breach context.[144]

---

141. See, for example, a letter from the Commander of U.S. Cyber Command Keith Alexander to Senator John McCain. Letter from U.S. Army Commander Keith Alexander to Senator John McCain 1 (May 3, 2012), https://publicintelligence.net/u-s-cyber-command-cybersecurity-legislation-position-letter [https://perma.cc/ERH7-FR76] ("Additionally, given DoD reliance on certain core critical infrastructure to execute its mission, as well as the importance of the Nation's critical infrastructure to our national and economic security overall, legislation is also needed to ensure that infrastructure is efficiently hardened and resilient. Recent events have shown that a purely voluntary and market driven system is not sufficient."); *see also* Palmer, *supra* note 17, at 297 (arguing that voluntary efforts and market forces might not lead to adequate security for critical infrastructure).

142. Sales, *supra* note 32, at 1511-1517; KERFOOT, *supra* note 138, at 5. Research conducted by McAfee in 2010 and 2011 revealed that many privately-owned companies poorly invest in cybersecurity, mainly due to financial reasons. While we acknowledge McAfee's interests in the outcomes of such research, it still provides some insights on cybersecurity in the private sector. *See* STEWART BAKER ET AL., IN THE DARK: CRUCIAL INDUSTRIES CONFRONT CYBERATTACKS 1 (2011), http://www.mcafee.com/in/resources/reports/rp-critical-infrastructure-protection.pdf [https://perma.cc/2V5V-8JDP]; STEWART BAKER ET AL., IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 13-15 (2010), http://img.en25.com/Web/McAfee/CIP_report_final_uk_fnl_lores.pdf [https://perma.cc/YFE8-LS5S] [hereinafter BAKER ET AL., IN THE CROSS FIRE].

143. KERFOOT, *supra* note 138, at 6.

144. For a literature review of this matter, see Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 264 (2011).

CI markets often face the above-mentioned problems, which undermine effective signaling (and, in turn, could lead to suboptimal levels of cyber security). Private CI operators are often public utilities, which operate with limited, if any, competition. In addition, switching utility providers is often cumbersome, difficult, and rarely done.

In theory, consumers could also signal their discontent by limiting their usage and not just by switching. Yet this form of signaling is unlikely to be effective. Consumers often consider the services provided by CI operators essential. Therefore, even after they acknowledge the risks of cyber attacks, consumers will not reduce their level of consumption. The inelastic demand curve often pertaining to this form of consumption could lead to even harsher outcomes; not only will firms ignore consumer discontent, they will be indifferent to the costs that successful cyber attacks might entail. CI firms could easily recoup these additional expenses by raising prices (which, even if regulated, are often premised on a "cost+" calculation – a cost that would rise given the need to repair that attack's damages). Therefore, the market-based argument fails to convince that the market alone will achieve necessary CI security.

It should be noted that this critique is somewhat context specific. For instance, not all CIs are monopolies. Wireless services, which surely fall in the CI category in today's economy, are offered by several carriers in every geographical location, have multiple infrastructures, and feature relatively reasonable switching costs.[145] In addition, monopolies are not fully immune from the consequences of cyber attacks. Service failure due to such attacks causes public outrage, ignites the press, and leads to political pressure and regulatory inquiries. All of these factors cause financial losses and even greater government intervention in operations—outcomes that firms surely dread.[146] Therefore, even monopolies are incentivized to invest in cybersecurity measures.[147] But such pressures are often insufficient.[148]

Yet another set of challenges impede the market and social dynamics that might prompt firms to adopt proper protective measures—

145. The United States currently features four national carriers with separate networks (Verizon, AT&T, T-Mobile, and Sprint) and a regional network (US Cellular) available at some locations. *See* Scott Webster & Jessica Dolcourt, *Before You Switch Wireless Carriers, Read This*, CNET (Feb. 3, 2016, 7:59 AM), http://www.cnet.com/news/comparing-wireless-carrier-plans-us [https://perma.cc/CRB6-V982].

146. For further information on the social and political aspects of monopolies, see generally ALBERT O. HIRSCHMAN, EXIT, VOICE AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970).

147. It is plausible that a monopoly could be indifferent to costs since it can pay off these costs from its consumers, and thereby will not be deterred from overinvesting in cybersecurity.

148. Sales, *supra* note 32, at 1517 ("[S]trategically significant firms in uncompetitive markets are less likely to adequately invest in cyber-security than ordinary firms in competitive markets.").

those related to asymmetric information. To engage in any form of the signaling dynamics noted above, consumers (or reporters or politicians) require a variety of information—that is, information regarding the existence of cyber attacks, the (inadequate) levels of protection implemented, and the damages caused. In most cases, such information is rarely available to anyone outside of the CI operator (below we examine whether even the CI operator itself holds sufficient knowledge on the subject).

Indeed, even while a CI operator's failure is likely apparent, the causes for these failures, especially in the digital context, are not. Naturally, companies are not keen on divulging such information; disclosure could damage their reputation, scare off customers, and increase their legal liability.[149] It might also improve the success of subsequent attacks.[150] In addition, signals of high quality security measures that a responsible CI might consider conveying might be futile, as they are commonly distorted by other market players generating false signals[151] and therefore may eventually be disregarded by consumers.

Moreover, merely sharing information about attacks and defenses is insufficient. Many customers are not equipped to properly analyze its meaning. Therefore, if we endorse such a market-based approach as a measure to assure sufficient levels of cyber protection, we need to ensure not only that the information is distributed, but also that it is comprehensible.

(2) **Negative Externalities:** In many instances, the damage from a cyber attack, and the lack of appropriate defense measures, create *negative externalities*.[152] This argument has two facets. First, while cyber-related attacks create costs and direct losses for firms, they cause greater damage to others—such as their consumers—which firms refuse to internalize, especially given the market failures previously discussed. Indeed, as noted, even though firms could recoup some expenses from consumers, successful attacks will still prove costly to the firms: for example, damage to their infrastructures (digital, ICT, and other) and reputation and even increased exposure to possible lawsuits–all costs which they indeed internalize. However, because CIs provide vital services, consumers suffer additional extensive secondary damages due to the loss of service which firms do not necessarily internalize.

---

149. ROSENZWEIG, *supra* note 138, at 162-63.

150. *See infra* note 158.

151. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1036 (2014) (demonstrating this claim while referring to the failure of TRUSTe to properly signal a high level of security) [hereinafter Bambauer, *Ghost in the Network*].

152. Negative externalities occur when the parties to a transaction do not internalize its cost and a third party bears it. *See* KERFOOT, *supra* note 138, at 12.

A response to this obvious argument is that firms might indeed internalize consumer damage as well (including secondary damages), given the signaling dynamic noted above and the potential loss of business and revenue. In other words, the threat of negative consumer signals resulting from CI security failures will sufficiently incentivize the CI to provide adequate protection and apply investments which are at least equal to the damages they caused their consumers. This response, as explained above, is problematic given the prospect of market failures. Yet even in markets that feature competitive CIs and low switching costs, an additional aspect of negative externalities must still be discussed.

The aggregate social harm of a successful CI cyber attack will most likely be higher than the aggregate harm to both the firm and its consumers. This is due to the multi-sectoral effects of CI damage; harm to one CI can lead to harm to another CI, and even subsequently harm to the latter's consumers as well. For instance, electrical shutdowns or communication failures could negatively impact many other CI operators (such as those providing water) and individuals (who cannot receive services from those without power or communications).[153] In such cases, the primary CI will not internalize the negative impacts from successful cyber attacks and thus will not be properly incentivized to prevent them.[154]

With only partial incentives in place, it is clear that CIs will not voluntarily provide adequate protection since they lack the requisite incentives to allocate financial resources to proper and sufficient cybersecurity measures. Furthermore, due to spillover effects, some companies will fail to adopt sufficient security measures in order to limit positive externalities to other firms (possibly, their competitors) that will benefit from them and 'free ride' on their efforts. Instead, firms would rather attempt to 'free ride' on the investment of others, benefiting from the 'herd immunity' resulting from their protective steps, or expect that any cybersecurity failings will be dispersed, and therefore, they will not be held accountable.[155]

(3) **Information and Expertise Deficiencies:** Suppose, for the moment, that firms are fully incentivized to meet optimal cyber-security standards and activities. Are they properly equipped to do so?

Arguably, CI operators possess the optimal level of *information* on their facilities, and accordingly, they should know how best to protect

153. TED KOPPEL, LIGHTS OUT: A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH (2015) (discussing in depth the risks of a cyber attack on the U.S. electric grid); ROSENZWEIG, *supra* note 138, at 162-63.

154. For a similar argument, see Sales, *supra* note 32, at 1508.

155. KERFOOT, *supra* note 138, at 6.

them.[156] While this could be true generally, it is not necessarily the case in the cyber context. As noted, cyber attacks possess unique characteristics—they can rapidly change their form and spread from one context to another.[157] Therefore, the most relevant information on the nature and frequency of cyber attacks is likely to be found with a wide range of CI operators, rather than held by one single operator. As a result, a single firm that operates alone based on its own information is likely to choose a suboptimal strategy, or level of protection.[158]

However, before calling for governmental regulation, our analysis must still proceed as we have not yet pointed to an incurable failure that requires such intervention. Prima facie, CI operators should be capable and possess independent incentives to recognize such information deficiencies are afoot and to act in concert to cure them. One such cure could be to establish joint networks for information sharing and notification of relevant alerts. If these joint ventures were to unfold, this information deficiency problem could be independently resolved.

However, there are serious concerns that such information deficiency will not be independently resolved without an external boost or mandate. Fearing confidentiality issues by divulging trade secrets and business models, CI operators may refrain from information sharing with competitors (even if information sharing would be potentially beneficial for all parties,[159] as each side could receive future warnings).[160] In other instances, companies may hesitate to share information with other CIs, foreseeing possible antitrust violations.[161] In addition, companies might fear civil litigation for privacy violations if personal consumer data is shared with other parties.[162]

---

156. *See* George Loewenstein et al., *Disclosure: Psychology Changes Everything*, 6 ANN. REV. ECON. 391, 397 (2014) ("Sellers also naturally know more about the products they market than do consumers.").

157. *See supra* Section II.B.

158. Note however, that some argue that information gaps are not crucial in protecting CI. *See* Derek E. Bambauer, *Sharing Shortcomings*, 47 LOY. U. CHI. L.J. 465, 468 (2015) [hereinafter Bambauer, *Sharing Shortcomings*].

159. *Cf. id.* at 466 (arguing that information sharing is overrated in cybersecurity).

160. Many CI operators might act irrationally or with bounded rationality. As some CI operators do not possess all relevant information and/or fully understand it, they might rely on heuristics. Such heuristics could be helpful in many instances, but could also lead to undesired outcomes. *See* KERFOOT, *supra* note 138, at 11-12. For more on law and market behavior, see generally Avishalom Tor, *Understanding Behavioral Antitrust*, 92 TEX. L. REV. 573 (2014).

161. *See generally* 15 U.S.C. §§ 1-27 (2012); *see also* Palmer, *supra* note 17, at 319-23 (describing the legal barriers for information sharing); KERFOOT, *supra* note 138, at 35-36 (noting that information sharing schemes have failed due to antitrust concerns, and explaining how this problem might be resolved).

162. *See* ANDREW NOLAN, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS 16 (2015), https://fas.org/sgp/crs/intel/R43941.pdf [https://perma.cc/3X7Z-Q824]. *But cf.* ROSENZWEIG, *supra* note 138,

Therefore, regulatory intervention may be appropriate, if only to encourage or enable a trustworthy system of information sharing. The information deficiency problem could be exacerbated not only by a lack of information in general, but specifically by companies' inability to receive information in a timely manner when executed voluntarily. As an attack on one CI might be a precursor of an imminent attack on another, external measures might be required to facilitate the speedy transfer of data in real time.

In addition to information deficiencies, private CI firms may lack the expertise required to properly evaluate cyber attack risks or implement necessary security measures and thus be unequipped to respond to cyber risks. In this specific context, the state arguably has an advantage and is perhaps in the best position to advise CIs.

Again, this argument is counterintuitive: seemingly, CI operators should be in the best position to possess (or at least, acquire) knowledge on how to run their *own* operations. Here again, the cyber context leads to unique outcomes. CI operators often fail to obtain this knowledge as it is highly technical, specific, and possibly linked to other government-related activities. It is often outside the scope of regular CI operator activities. To illustrate, note that even Google, at least in some instances of cyber attacks, has reportedly requested the assistance of governmental agencies.[163] If this is true of tech-savvy firms such as Google, it likely applies to CI operators at the low-tech end.

Thus far, we have presented several arguments regarding market failures and other impediments that potentially prevent CI operators from optimizing their defenses against cyber attacks. To resolve such challenges, we offer several possible courses of action. In the next Part, we begin by proposing modest solutions that feature limited intervention while maintaining a market-based approach to the challenges of protecting CI from cyber risks. To some extent, this analysis explains the rationale behind recent steps taken in the United States and elsewhere to promote CIP. However, as we further show, a limited approach is not an optimal strategy to promote CI sustainability and security.

B. Limited Intervention via Disclosure Requirements and Information Sharing

As previously mentioned, a lack in information creates a substantial barrier to optimal market-based cybersecurity. This gap has two

---

at 168 (doubting that such issue presents real difficulties to companies); Bambauer, *Sharing Shortcomings*, *supra* note 158, at 469-72 (rejecting assumption that legal liability impedes companies from sharing data).

163. As Paul Rosenzweig describes, when Google encountered a cyber-attack, they approached the National Security Agency (NSA) to aid them. *See* ROSENZWEIG, *supra* note 138, at 158.

prongs: one pertaining to those outside the firm who fail to understand the risks the firm's responses (or lack thereof) to cyber threats create, and the other pertaining to the firm itself and its inability to properly respond to attacks given insufficient information and expertise. Various policy strategies could be (and in some contexts, have already been) implemented to eliminate these barriers. If successful, market-based solutions that only call for limited intervention could still prevail (assuming that the other concerns noted above are addressed as well—an issue we discuss in subpart C). As we now explain, this is easier said than done.

1. Bridging the Information Gap: Disclosure Requirements to Consumers

A simple response to the fear of insufficient political and social signaling by the public, in light of CI cyber failures, due to the public's lack of proper information and understanding of related issues, would be to enhance disclosure via mandatory disclosure rules. This requirement is closely related to the broadening theme of 'disclosure regulation,'[164] which has been established in a variety of contexts. On its face, the notion of establishing such disclosure rules could hardly be contested, as it echoes similar requirements in the related context of securing personal information.[165] In this latter context, when learning of a personal data breach, businesses are required to notify those potentially affected by it (such as those to whom the personal data pertained).[166] Similarly, in the CIP context, it may be wise to establish disclosure regulations for CI operators. These disclosures would apply to cyber attacks attaining a certain degree of success. For instance, regulators could oblige CI operators to notify their customers of any damage to their infrastructure or of any service disruption cause by a cyber attack.

While this solution seems both relatively harmless and easy to implement, it is unclear whether such steps are wise. Disclosure could

---

164. Cass Sunstein articulated the phrase "regulation through disclosure." *See* Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613 (1999).

165. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 920, 932-35 (2007). There are various explicit regulations for data security in the United States. For example, "[T]he Gramm-Leach-Bliley Act (GLB Act) requires financial institutions to develop procedures for protecting the security of customer data and empowers the Federal Deposit Insurance Corporation . . . and other bank regulatory agencies to promulgate data security regulations." *Id.* at 920; Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501, 505, 113 Stat. 1338, 1436-37, 1440-41 (1999) (codified as amended at 15 U.S.C. §§ 6801, 6805 (2012)).

166. See, for example, the first type of such regulation in California: CAL. CIV. CODE §§ 1798.28, .82, .84 (West 2016).

achieve very little and generate needless costs. Indeed, disclosure-based regulations in general have been widely criticized,[167] specifically regarding the high occurrence of such disclosures and their potential inaccuracies. Cyber attacks occur frequently, but their effects are often minimal and therefore the abundance of disclosures and notices might backfire. In addition, consumers could underestimate the scope of this problem due to a cognitive bias.[168] With time, these notifications might be considered untrustworthy or unnecessary, and fail to receive proper attention, if any.[169] In addition, mandatory disclosure mechanisms could leave serious shortcomings unreported, such as vulnerabilities that have not yet been abused. Therefore, disclosure regulations alone cannot bridge the existing information gaps between consumers and CI operators.

A different strategy could resolve these shortcomings. Instead of focusing on incidental damages, disclosure mechanisms could focus on risks. Hence, disclosure mechanisms could oblige CI operators to publicly report security measurements and/or security test results.[170] It would be a one-time form of disclosure, not spread over time or provided in a manner which could desensitize recipients.

However, this second disclosure model poses risks of its own. It does not resolve issues related to the possible underestimation of risks that have yet to materialize, and thus does not fully account for the importance of security measures.[171] Yet more importantly, such reports could exacerbate the risks of cyber attacks because they divulge CI vulnerabilities.[172] Therefore, even if such a model could potentially aid cybersecurity, it could also harm it; this model is consequentially suboptimal.

---

167. *See* KERFOOT, *supra* note 138, at 18-19.

168. Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOMM. & TECH. L. REV. 303, 313 (2008); Neil D. Weinstein, *Optimistic Biases about Personal Risks*, 246 SCI. 1232, 1232 (1989).

169. Schwartz & Janger, *supra* note 165, at 916; Fred H. Cate, *Another Notice Isn't Answer*, USA TODAY (Feb. 27, 2005, 8:23 PM), http://usatoday30.usatoday.com/news/opinion/2005-02-27-consumer-protection-oppose_x.htm [https://perma.cc/NZ89-H97Y].

170. *See, e.g.*, Letter from U.S. Army Commander Keith Alexander to Senator John McCain, *supra* note 141, at 3 ("The proposed security requirements in the Administration's proposal would not dictate specific measures that may become outdated, but rather would require critical infrastructure to achieve security results using methods of their choice.").

171. Bambauer, *Ghost in the Network*, *supra* note 151, at 1031 ("Consumers have difficulty detecting whether firms have made improvements to cyber defenses, leading to reluctance to pay a security premium.").

172. As we further argue, this claim might be false, as exposure could actually improve cybersecurity. *See infra* Section V.B.4. Note that even if a patch (a piece of software code repairing the security problem) is introduced together with the vulnerability report, problems might follow as the relevant entities might be too slow in applying this patch.

2. Fixing Information and Knowledge Gaps

We now turn to discuss failures relating to CI operators' ability to collect information and obtain knowledge on cyber attacks. In the face of these challenges, global regulators have acknowledged CI operators' information and knowledge gaps and have offered various mechanisms, with minimal intervention, to resolve this issue.

A centrally proposed model introduced the CERT (Computer Emergency Response Teams) to mitigate information deficiencies. CERT features voluntary mechanisms to coordinate cyber information sharing between relevant governments and firms (including CIs), as well as between firms themselves.[173] In this manner, firms receive up-to-date information on cyber threats in real time.[174]

Again, incentives are an issue: Some CIs may lack the necessary incentives to share critical information with CERT (which could encourage 'free-riding' by providing access to incident-related information without the need to contribute). Therefore, supplementary measures are required. One relatively moderate set of measures includes granting safe harbors and immunity to companies that share information of a certain extent and degree with CERT.[175] With such measures in place, these firms will not fear civil litigation resulting from such sharing, given potential breaches of users' privacy.[176] Note, however, that applying a safe harbor carries with it the risk that firms will share information strictly within its confines, rather than take a chance and broaden their sharing activities, out of fear that liability will immediately follow. Thus, the safe harbor must be constructed carefully. A more radical solution mandates that CI operators report cyber attacks in real-time.[177]

Let us now turn to *knowledge* deficits. To some extent, government initiatives that generate knowledge and enable information sharing between firms could bridge the gap. Not surprisingly, there are various

---

173. See, for example, the US-CERT at https://www.us-cert.gov/about-us.

174. Some scholars argue that a majority of states find information sharing highly important for cybersecurity. *See* Shackelford & Kastelic, *supra* note 64, at 20 ("[T]he percentage of nations referencing reporting and sharing cyber threat information along with best practices was 64 percent . . . .").

175. See discussion in Kesan & Hayes, *supra* note 33, at 1530.

176. ROSENZWEIG, *supra* note 138, at 169. Perhaps, to reduce chances of possible privacy violations, the state should not have access to such information. *But see* Bambauer, *Sharing Shortcomings*, *supra* note 158, at 469-72 (arguing that information sharing incentives are not required as firms will be motivated to do so); KERFOOT, *supra* note 138, at 34.

177. For a different analysis of this issue, see discussion in Kesan & Hayes, *supra* note 33, at 1539-54 (applying literature pertaining to voluntary and mandatory information sharing in other contexts to the specific cyber-related context).

initiatives around the world, including in the United States,[178] supporting this dynamic. One such initiative is standardization,[179] a process through which relevant firms and other stakeholders (including government entities) negotiate to determine an acceptable response strategy and practice to cyber attacks on CI. At times (as noted in the discussion above about the role of the NIST),[180] government intervention could facilitate the standardization process. If several standards are formed, the government could indicate which standard it prefers.[181] Another initiative creates partnerships, enabling collaboration between CI operators and cybersecurity companies, and among CI operators themselves.

C. Limited Intervention via Internalizing Externalities/Ex Ante Regulation and Incentives

Even if we were able to overcome the information and knowledge gaps, we would still be left with the problem of externalities, which leads to underinvestment in cybersecurity. Therefore, mechanisms need to be developed to ensure internalization of the damages of cyber attacks by CIs. Or at least, additional steps must be taken to further incentivize CIs to enhance cybersecurity efforts. Let us now examine two strategies that do this.

To overcome externality-related problems caused by cybersecurity risks, the regulator can enact regulation imposing liability on CI operators through tort law in regard to harms caused by successful cyber attacks.[182] Another strategy is to impose administrative fines or even criminal liability on companies and/or their executives following CI failures that inflict damage. While these measures affect the CI after the risks have materialized and the damage has been done (i.e., ex post), they still might prove effective. In order to prevent liability and its consequences, CIs will act proactively and initiate measures that prevent their liabilities, be they tort, monetary fines, or criminal. Thus, these measures are clear examples of state intervention to regulate behavior of private parties ex ante by incentivizing preventive and precautionary steps to limit risk. These forms of regulation could be limited in their intrusiveness, but their effectiveness in this context is somewhat questionable.

Analytically, the success of such an ex post regulatory model relies on two implicit assumptions: (1) Ex ante conduct of the relevant entities can be sufficiently altered (in this case, CIs will implement proper cybersecurity measures) by imposing ex post liability, and (2) state

178. KERFOOT, *supra* note 138, at 33 (referring to HSPD-7).

179. The NIST is a good example of standardization. *See supra* Section III.A.1.

180. *See supra* Section III.A.1.

181. KERFOOT, *supra* note 138, at 38.

182. ROSENZWEIG, *supra* note 138, at 173; KERFOOT, *supra* note 138, at 14.

agents (legislature, regulators, and/or courts) can identify, establish, and enforce a proper standard of conduct for these firms after the fact. These two basic assumptions are acceptable in many instances, but the cybersecurity context presents unique challenges that could reduce the efficacy of this ex post strategy.

As noted, one of the central motivations for imposing and enforcing ex post liability is to deter ex ante activity. In this specific context, ex post liability is imposed upon CI aggressors[183] in an effort to curb such attacks and possibly on the CI itself, which failed to properly protect itself (again, to deter CIs from applying lax standards of protection).[184] Before proceeding to discuss CI liability, let us add a few words regarding direct liability on the attackers. It is quite clear that establishing (even harsh) liability rules against CI attackers does not and will not sufficiently protect CI from cyber attacks[185] These attacks are difficult to identify and even more difficult to litigate and prosecute. Thus, CI attackers are insufficiently deterred.

Therefore, let us focus on ex post deterrence of CI operators to motivate them into adopting proper cyber security measures. Here too, we should remain skeptical of this scheme's success. At the ex ante stage, CIs may not significantly fear the prospect of ex post sanctions. The prospects of cyber threats materializing (if adopting lax security measures) are uncertain. Even if an attack were to occur, it would be difficult to pin the blame on the firm and prove that it resulted from the CI's negligence.[186] It is thus unlikely that ex post liability will motivate or incentivize CIs to applying proper security measures.

Let us elaborate on this thought further: Remember, the particular characteristics of cyber attacks make assigning blame and attribution

---

183. An example of such method can be traced in the United States. In 2015, President Barack Obama issued a new Executive Order that "empower[s] the administration to apply sanctions against individuals and groups that threaten the nation's critical infrastructure through malicious activities in cyberspace." Aaron Boyd, *Obama Signs Order Authorizing Sanctions Against Cyber Criminals*, FED. TIMES (Apr. 1, 2015), http://www.federaltimes.com/story/government/cybersecurity/2015/04/01/obama-executive-order-sanctions-cyber-criminals/70770684 [https://perma.cc/EG3G-QANN]; *see also* Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 2, 2015).

184. For more on deterrence and economic analysis of crime, see generally Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968). Note that, generally speaking, deterrence theory had been widely criticized over the years. *See, e.g.*, Dan M. Kahan, *The Theory of Value Dilemma: A Critique of the Economic Analysis of Criminal Law*, 1 OHIO ST. J. CRIM. L. 643, 643-47 (2004).

185. Mark Grady & Francesco Parisi, *The Law and Economics of Cybersecurity: An Introduction*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 1, 1 (Mark F. Grady & Francesco Parisi eds., 2006) ("Cybercrime . . . is highly resistant to the usual methods of prevention and deterrence.").

186. For a similar argument regarding cybersecurity, see generally Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 DAEDALUS 70, 73-74 (2011).

in the cyber realm difficult[187] or there could be various entities that have jointly caused the failure in the CI protection as well as the claimed damages.[188] The court (or the legislature) will be required to decide on highly complex questions regarding the scope of the direct and/or indirect economic consequences that are actionable, and to decide who has legal standing to claim such damages.[189] The expected complexity of such decisions, and the extended time such proceedings take, might again undermine deterrence.

Perhaps enacting harsher ex post measures against CI operators for security breaches—such as criminal liability against executives—could offer a solution.[190] However, strict requirements could potentially backfire. They might set a disproportionally high standard of behavior for worthy players in the field, leading to undesired exits by capable individuals and their firms, who will not want to risk criminal liability. Therefore, the use of this drastic measure should be limited.

Yet perhaps an even greater challenge in regulating CIs ex post in the cyber context is establishing and enforcing the liability standard after the fact.[191] As noted, according to this ex post regulatory model, the state does not require CI operators to adhere to cybersecurity standards which are examined ex ante. With that, a CI operator who does not ex ante implement proper standards could be held liable in court if an attack unfolds and damage is caused.

Defining liability in this context is complex, but nonetheless critical for this model to succeed. Courts are obvious candidates for setting liability standards—a difficult and arduous task. Deciding after the fact whether a specific CI's conduct met a reasonableness standard will generate very vague messages and rules for CIs contemplating the form of system and method to implement. In addition, judges might lack the sufficient expertise to make such rulings in this highly technical context. Errors in the process will undermine its success. To resolve both problems, courts could rely upon a set of standards endorsed by the state; meeting this standard, therefore, would provide a safe harbor for CI operators and immunity from liability. In that way, it could de facto

187. *See* KERFOOT, *supra* note 138, at 16; *see also supra* note 26.

188. On this matter, we can separate "joint and several liability" as a possible solution to the attribution problem. *See* KERFOOT, *supra* note 138, at 39. For a discussion of the challenge of applying the "economic loss" doctrine from tort law, which confronts the difficulties of establishing the extent of claimed damages in the cyber-security context, see generally David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935 (2016).

189. ROSENZWEIG, *supra* note 138, at 172.

190. KERFOOT, *supra* note 138, at 15.

191. ROSENZWEIG, *supra* note 138, at 173.

become a mandatory standard for CI operators.[192] Below we discuss the challenges government entities face in setting such standards;[193] yet briefly note here that such practices are highly problematic and there is a good chance they will not lead to an optimal outcome.

To summarize, ex post internalization models raise many analytic difficulties and are unlikely to lead to an acceptable regulatory response to the cybersecurity challenge. We concede that liability rules might be fitting in this context for various ethical reasons, and as a means of promoting distributive or corrective justice. Yet these issues are beyond our current inquiry.[194] It is also noteworthy that a possible solution to the challenges discussed here is a functioning cyber-liability insurance market.[195] If CI operators were able to purchase insurance for all damages caused by cyber attacks, insurance companies would be charged with confronting (successfully or not) cybersecurity challenges. Insurance companies would monitor the actions of various relevant entities, determine standards for action, and update them according to the progress of technology and the realization of the risks.[196] These insurance markets are still in their infancy.[197] Therefore, this aspect must be revisited in the future.

The ideas we discuss directly above focus on measures to internalize negative externalities, which have proven to be ineffective. We can approach the issue from a different avenue: by providing direct and indirect incentives to CI operators who sufficiently adapt to cyber challenges.[198] Incentives can take the form of direct payments for meeting cybersecurity standards,[199] a right to participate in government tenders,[200] or tax benefits based on criteria related to cybersecurity measures. In addition

192. Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 314 (2015).

193. *See infra* Section V.B.

194. For more on liability, see generally George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 HARV. L. REV. 537 (1972).

195. ROSENZWEIG, *supra* note 138, at 173; KERFOOT, *supra* note 138, at 19-20.

196. ROSENZWEIG, *supra* note 138, at 173; Opderbeck, *supra* note 188, at 973-74.

197. For a literature review on this issue, see SASHA ROMANOSKY, DOCKET NO. 130206115-3115-01, COMMENTS TO THE DEPARTMENT OF COMMERCE ON INCENTIVES TO ADOPT IMPROVED CYBERSECURITY PRACTICES 4 (2013), https://www.ntia.doc.gov/files/ntia/romanosky_comments.pdf [https://perma.cc/9EDX-GDHB].

198. KERFOOT, *supra* note 138, at 21.

199. Bambauer, *Conundrum*, *supra* note 21, at 658-59.

200. Derek Bambauer proposes using "the carrot and the stick" approach. *See* Bambauer, *Ghost in the Network*, *supra* note 151, at 1018; *see also id.* at 1062-78 (describing approach); KERFOOT, *supra* note 138, at 20-21 (advocating providing direct incentives and the use of government procurement).

to incentivizing their implementation, the state could provide cybersecurity tools and assistance to CI operators without charge.

However, such direct incentives also insufficiently incentivize implementing adequate CI cybersecurity measures. Even with such incentives in place, some CI operators might decide that their implementation is not worthwhile after considering the potential costs of applying such protective measures and their interference with CI operations. Furthermore, this type of policy may face political opposition. The public, who in many cases is dissatisfied with public utilities/private CIs, may oppose the redirection of its taxpayer money to these firms' pockets for services the CIs are expected to provide and that are already paid for. And again, the success of the model relies on the state's ability to set cybersecurity standards and monitor their implementation—a practice that, as we shall see shortly, generates substantial problems.

To conclude this Section, the ability to create a market-based regulatory regime, which is supplemented by mere disclosure obligations, knowledge transfers, tailored incentives, or ex post regulation, is unsatisfactory.[201] Therefore, it is necessary to consider other mechanisms to drive companies to implement proper cybersecurity measures, such as ex ante regulations mandating specific steps.

V. MODELS OF CIP: EX ANTE REGULATION

A. Direct Governmental Intervention: Strategies and Benefits

Our discussion thus far has focused on regulatory strategies premised upon market-driven outcomes, with the state engaging in limited interventions when market and social forces are destined to fail. In this Part, we examine the opposite side of the regulatory spectrum—a CI cybersecurity regulatory scheme that is premised upon direct government supervision. Here, the state regulates and determines which defense mechanisms CI operators must adopt, enforces their implementation, and monitors compliance.[202] These activities would most likely be undertaken by a designated state agency that would collaborate with other governmental security agencies to obtain information on offensive and defensive cyber measures and thus increase its success. As discussed below, the overall scheme might be cloaked, at least partially, in secrecy.

While this regulatory scheme is a far cry from the current U.S. approach, it is nonetheless important to consider. As noted, several countries have already implemented similar strategies, and it is possible

201. For a similar stand in the United States, see Clayton, *supra* note 107.

202. For a discussion of a similar option, see Kesan & Hayes, *supra* note 33, at 1545-46 (requiring the entities posing the highest risk to adopt NIST standards).

that others will follow.[203] Furthermore, regulating the means by which CIs are protected from cyber attacks, resulting from terrorist acts or acts by hostile nations, seemingly fits within the state's overall role of protecting citizens from attacks and hostilities—a task not commonly assigned to the private sector.[204] In addition, a discussion of this option allows for an overall analysis of other regulatory measures. The result of this discussion, when integrated with the discussions noted above, formulates an optimal framework, which we present in Part VI.

A government-centered regulatory scheme could be implemented using several measures: direct, mandatory legislation that maps out the bodies subject to it and their obligations, or a licensing regime that requires CI operators to be licensed and that has various cyber-related obligations and requirements. The analysis below discusses government-centered regulation in principle, regardless of the specific means selected.

Government-centered regulation has several advantages, many of which are the mirror image of the shortcomings of the market-based schemes discussed above. Above all, this model provides a simple response to the problem of limited incentives for meeting cybersecurity standards. Here, the standards are set by the state, which also enforces and monitors their implementation. Furthermore, concerns regarding information and knowledge deficits and gaps could also be resolved. The government can serve as a central hub for both information and knowledge. Because the government would receive and handle all relevant cyber attack information, the government-centered scheme would overcome the business and legal constraints mentioned in our analysis on the market-based model. Furthermore, the government can integrate into this process additional information to which it is privy, i.e., information received from its military and intelligence agencies.[205]

Similar advantages can be realized regarding the production and flow of knowledge and expertise. The state is well situated to acquire relevant expertise regarding cyber attacks and defenses by recruiting relevant experts who can continuously advise on defensive measures that will be distributed to all CI operators. Here again, the government could integrate insights from other security and intelligence agencies taking part in cyber defense (and even offensive) initiatives, without the risk of compromising state secrets or intelligence assets.

---

203. *See supra* Section III.B.

204. *See* BAKER ET AL., IN THE CROSS FIRE, *supra* note 142, at 26 ("You wouldn't go to a post office and ask them how they're tending to their own ballistic missile defense . . . but that is the equivalent of the current set-up in cybersecurity." (quoting General Michael Hayden)).

205. For example, Ajay Banga, president of MasterCard Worldwide, stated, "We need help from government that only government can provide, including intelligence information to counter growing threats." *See* Clayton, *supra* note 107.

Beyond these noted advantages, direct government regulation enables two additional features to enhance the efficiency of CI protection and confers unique benefits for the cyber context: *secrecy* and *concentration* (or *centralization*). A government agency can engage in framing and enforcing cyber strategy in relative secrecy. In the cyber context, secrecy can prove beneficial, as knowledge of security measures can be exploited by potential attackers to increase their chances of success.[206] Secrecy, therefore, promotes security.[207]

A governmental-driven regulatory scheme also allows for *concentration* of information, knowledge, and decision making within one entity. Of course, an abundance of regulators could be vested with regulating CIs.[208] This situation is less than ideal. When authority is divided between several regulators, each authority might act to increase its power at the expense of the other, causing a power struggle between the various agencies. This could lead to poor decision making and inefficiency.[209]

B. Shortcomings and Risks of a Governmental-Centric Approach

1. Ex-Ante Regulation and Optimizing Knowledge

The noted advantages of direct regulation of CI cyber risks seem to resolve many of the concerns noted in previous Sections. Yet, with these advantages come other problems. And while the global trend may be toward state-centric protection of CIs, many scholars and policymakers argue that this regulatory trajectory is unwise. Some find the claim that a single government entity "can micro-manage every aspect of cybersecurity and dictate best practice[s] is hubris."[210]

---

206. Peter P. Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, 3 J. ON TELECOMM. & HIGH TECH. L. 163, 167 (2004) (arguing that secrecy could be "an essential tool for enhancing security"). But as we further show, others argue that "there is no security through obscurity," i.e., that revealing details could actually improve security. *Id.* (footnote omitted).

207. Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y REV. 281, 294 (2014) ("Even if we understand that the national security establishment can make mistakes, there remains the argument that secrecy is vital to security; that the price of transparency is too high.").

208. A non-centralized governmental approach, i.e., granting authority to multiple agencies, could be problematic due to plurality of regulators. Much like in the U.S. approach to CIP, lacking a single authoritative source for coordinating and notifying CI operators might lead to confused CI operators, inconsistent messages, and moreover, uncoordinated federal efforts. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-628, CRITICAL INFRASTRUCTURE PROTECTION: KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS NEED TO BE CONSISTENTLY ADDRESSED 15 (2010), https://www.hsdl.org/?view&did=20017 [https://perma.cc/S4GS-U859].

209. KERFOOT, *supra* note 138, at 25-26, 29.

210. *Id.* at 32.

One powerful set of critiques points to the inefficiency of the government-led regulatory scheme. These critiques state that government entities are not the optimal custodian and aggregator of knowledge in a cyber context.[211] Quite to the contrary, it is more likely that knowledge generated and held by the state will prove to be subpar.[212] Intuitively, in technological contexts, expertise lies mainly with external and diverse experts rather than the central government. The state can hire experts and learn from them, but so can private companies. There are no guarantees that the state will know which experts to listen to. Indeed, the state might be highly motivated to objectively choose the best solutions (we reconsider this notion below),[213] but its lack of expertise could affect its choice and lead it to select a suboptimal strategy.

Beyond this general concern with the government's inability to obtain relevant knowledge, we critically assess five specific shortcomings that pertain to various technological aspects of the cyber protection context. *First*, scholars opine that the negative impact of a government-led regulatory model could extend well beyond the level of CI protection required, and affect aspects of cyber research. When the state, rather than the market, dictates conduct, this might affect overall innovation in the field.[214] Innovation will be steered toward the specific issues government deems interesting, rather than naturally developing in an optimal direction. But an important caveat is due. Cyberspace is developing rapidly; state influence may be minor and narrowly focused. Thus, innovation could proceed without substantial interference.

Second, even if the state were capable of establishing a reasonable blueprint to respond to cyber threats, it would have more difficulty in updating and amending this blueprint due to the fast pace of the constant, overall changes in the cyber field.[215] The realm of cyber risks is highly volatile, and quick responses are necessary. In other fields, the fact that policy changes take time might not lead to devastating outcomes. It might even enable better policymaking, as it allows for responsible decision making after in-depth consultation. This is not true for the cyber realm, which is arguably unique in that it is constantly

211. *Id.* at 38; Michael J. O'Neil & James X. Dempsey, *Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry*, 12 DEPAUL BUS. L.J. 97, 111 (2000) (arguing that in information security standards, "the private sector may well be ahead of most government agencies").

212. ROSENZWEIG, *supra* note 138, at 163-64.

213. *See id.* at 163.

214. KERFOOT, *supra* note 138, at 9-10.

215. Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 241 (2010).

undergoing change.[216] For example, a powerful critique of the FERC standard-setting process in the energy market featured a slow-moving process, in which an updated standard was retracted at the time of its approval because it was already outdated.[217]

Third, state monitoring and enforcement could lead to an undesirable practice of 'box checking' or 'box ticking.'[218] When responsibility rests on the shoulders of the state to set standards for cyber defense, some corporations will simply comply without further examining whether such protection is optimal. Therefore, greater involvement of relevant players in the process is necessary. Note that this critique also pertains to other instances in which the defense standard is set by external (even commercial) parties.

Fourth, recent trends in the technological practices of private companies tend to further minimize the benefits of governmental regulation. In the past, such companies, including private CIs, relied upon proprietary software—computer code written specifically for them. However, financial and compatibility concerns pressured many companies to switch to Commercial, Off-The-Shelf (COTS) software.[219] This transition offers advantages and disadvantages for cybersecurity that are beyond the scope of our analysis.[220] However, this change has clear implications for our current discussion; with COTS, specific governments have less of an advantage in identifying and resolving cyber threats. Here, the global commercial market is faced with similar challenges, and it is likely that expertise lies there.

Finally, and perhaps most importantly, the state-driven and mandated mechanism of CI cyber defense is only meaningful when coupled with effective enforcement. Arguably, the state could impose various sanctions against companies that fail to comply, including requiring that they cease operations (note the authority vested with the DHS in

---

216. *See* Ben Dipietro, *Speed of Tech Change a Threat to Cybersecurity*, WALL ST. J. (Mar. 17, 2015, 9:52 AM), http://blogs.wsj.com/riskandcompliance/2015/03/17/speed-of-technological-change-is-a-threat-to-cybersecurity [https://perma.cc/Z2JK-DRUZ]; SYMANTEC WHITE PAPER, CYBER SECURITY FOR FINANCIAL SERVICES: STRATEGIES THAT EMPOWER YOUR BUSINESS, DRIVE INNOVATION AND BUILD CUSTOMER TRUST 2 (2015), https://www.symantec.com/content/en/us/enterprise/white_papers/cybersecurity-whitepaper-financial-wp-21352892.pdf [https://perma.cc/ART7-EXHF].

217. *See supra* Section III.A.2, specifically the discussion in *supra* note 99. However, it is notable that secrecy could improve the government's ability to deal with rapid changes more quickly.

218. *See* Palmer, *supra* note 17, at 348, 364 (arguing that setting minimal standards could lead to more harm as utilities might strive to only merely meet them).

219. *See* CLARKE & KNAKE, *supra* note 139, at 140.

220. Generally, COTS operating systems increase connectivity between CIs' control systems, but at the same time, increase their overall vulnerability. *See* Stig Johnsen et al., *Reducing Risk in Oil and Gas Production Operations*, *in* CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 19, at 83-84.

the chemical sector), or terminating their CI license.[221] However, enforcement is not easily achieved since it requires substantial resources. The FERC's experiences in enforcing cyber defense standards illuminate the difficulties in enforcing such standards with government-budgeted manpower and resources.[222] Furthermore, in many cases, private CIs that are subject to regulation are powerful entities that are not easily penalized by the regulator (certainly not severely—after all, they control a *critical* infrastructure). Notably, even without enforcement, a government-based approach could increase knowledge and improve information sharing in real time, but such goals could be achieved while applying more lenient, and even optimal, measures.

2. State Regulation, Knowledge Gaps, and External Considerations

When the state chooses standards that apply to the entire CI market, fears of regulatory capture and undue influence come into play, as do concerns of the impact of other external considerations.[223] Indeed, authorizing the State to set cyber-security standards that bind private CIs brings about known dangers which come with governmental interventions. In this context, such concerns could have substantial and specific negative consequences. In addition, the government will turn to external bodies for advice, and external counsel is in fact useful.[224] Particularly regarding cyber issues, the government needs all the help it can receive. But there is a thin line between desirable consultation and unacceptable undue influence. In the cyber context, it is reasonable to expect this line will be crossed. Moreover, options for effective oversight, which could mitigate problematic practices, are limited. These substantial concerns are relevant and need to be accounted for. They could even lead to a decision to opt against extensive governmental intervention.

Two separate interests have the potential to cloud the regulator's judgment: those of *technology companies* and *sectoral competitors* of private CIs. Each form of influence leads to two different forms of concern: suboptimal levels of protection and the negative impact on competition and consumers.[225]

---

221. *See supra* Section V.A.

222. *See* Court, *supra* note 97, at 454.

223. While regulatory capture could lead to suboptimal protection, some scholars argue that it could actually advance the public interest. *See, e.g.*, Lawrence G. Baxter, Essay, *"Capture" in Financial Regulation: Can We Channel it Toward the Common Good?*, 21 CORNELL J.L. & PUB. POL'Y 175, 175-76 (2011); Dorit Rubinstein Reiss, *The Benefits of Capture*, 47 WAKE FOREST L. REV. 569, 572 (2012).

224. Reiss, *supra* note 223, at 590-92, 607.

225. David Thaw addresses the concerns of regulatory capture in the cybersecurity context. He describes a specific environment in which regulatory capture did not undermine the

The first, more intuitive concern pertains to lobbying and other forms of pressure applied by cyber tech firms. According to public choice theory, companies and interest groups have a clear incentive to pressure the regulator to choose favorable measures and standards that are the most profitable for them.[226] As such, lobbying initiatives could persuade government officials to select technologies and cybersecurity firms based on lobbying strength, not objective measures relating to optimum security. Here, implications of this selection could prove dire, as this dynamic could lead to inferior levels of protection. However, the consequences of effective lobbying do not need to be so dramatic. It is more likely that the sole harm of the public choice dynamic will be inefficiency, as the regulator will choose superfluous security measures that create unnecessary costs for CIs, which will ultimately roll them on to consumers or lead CIs to cut costs elsewhere and refrain from providing vital services. Furthermore, the complexity and relative opacity of the cyber context complicates public oversight of these processes[227] and allows lobbying forces to take their toll, thus exacerbating this problem.

The second concern is more complex and addresses problematic competitive maneuvering among private CIs and other firms. In their efforts to gain a competitive edge, firms often strive to burden their rivals with regulatory obligations. We refer to this form of problematic influence as *regulatory incitement*; a process by which interest groups (often under the guise of legitimate concern to protect the state or consumers) aim to convince regulators to adopt standards that negatively affect their competitors, and might, in fact, be unnecessary. The negative effect could be a financial encumbrance upon the competitor, or it can prove to be a technical nuisance that diverts the firm's attention and resources. In the cyber context, this might occur when interested parties convince the government to encumber various CIs with unnecessary cyber protection measures to create costs and slow down operators.

This last assertion may, at first, seem to result from mere paranoia. However, regulatory incitement concerns are based on past events. One good example of this is when citizens (or perhaps those with vested interests) pressured the Federal Communications Commission

---

fairness and efficiency of the regulatory process in the context of data security. Note however, that he lists several requirements essential for this positive dynamic to unfold, which are not fulfilled in the context here discussed. David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 371 (2014).

226. On modern public choice theory, see JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT: LOGICAL FOUNDATIONS OF CONSTITUTIONAL DEMOCRACY (1965); DENNIS C. MUELLER, PUBLIC CHOICE II: A REVISED EDITION OF *PUBLIC CHOICE* (1989). In this context, see ROSENZWEIG, *supra* note 138, at 163; KERFOOT, *supra* note 138, at 7; *see also* Thaw, *supra* note 225, at 335 (discussing various definitions of "regulatory capture").

227. *See infra* Section V.B.4.

(FCC) to ensure new cellular and Internet telephony provided emergency communication capabilities (specifically, location identification functions). While critically examining these incidents, Susan Crawford warned that the real motive behind the regulatory-driven technology requirements was pressure by wireline/telecom giants to slow down and delay rising competing forces through regulations that imposed extra costs on them.[228] In other words, wireline/telecom giants engaged in regulatory incitement.

A critical reader might argue that regulatory incitement is not applicable to our current discussion on CI cybersecurity, which does not focus on competition between monopolies and upcoming forces, but rather among monopolies themselves. In such a case, a specific firm's effort to convince the regulatory body to add burdens to its competitors would be of little use, as these additional burdens will be quickly applied to the firm itself, thus eliminating the competitive advantage. But the dynamic nature of markets renders the regulatory incitement argument relevant nonetheless. New players are constantly entering the markets and competing against existing CI owners (for instance, consider renewable energy providers or novel models of spectrum communication). Therefore, such concerns should not be taken lightly. To some extent, they unfolded during the negotiations in Europe regarding the final language of the NIS Directive and the definition of "Digital Service Providers," which are subjected to some regulatory requirements. Here, for instance, social networks were excluded from the final version while search engines were not.[229] This discussion further illuminates how vesting the government with the power to decide on the technological standards private firms must implement can lead to suboptimal outcomes with potential harm to consumers and a failure to prevent CI cyber risks.

3. Constitutionality, Human Rights, and Legality

State actions are scrutinized according to their legality, constitutionality, and impact upon individual rights; cyber risks are not exceptional. A full discussion of this aspect justifies (at least) a separate article. At this juncture, we merely strive to map out possible points of tension between this regulatory approach (of extensive governmental intervention in the cyber-regulation of CI) and individual rights.

---

228. Susan P. Crawford, *The Ambulance, the Squad Car, & the Internet*, 21 BERKELEY TECH. L.J. 873, 904-11 (2006).

229. *See* Aline Doussin, *New EU Cybersecurity Requirements Soon to Fall on "Essential Services" Operators*, SQUIRE PATTON BOGGS: GLOBAL IP & PRIVACY L. BLOG (May 29, 2016), http://www.iptechblog.com/2016/05/new-eu-cybersecurity-requirements-soon-to-fall-on-essential-services-operators/ [https://perma.cc/V4WW-BM54].

We begin by examining the relatively simple aspects. Closely regulating CIs' actions encumbers their property rights, as well as some aspects of freedom of occupation.[230] In terms of property, many CI operators are private entities; thus, any obligations, restrictions, and costs could negatively affect their property rights. Indeed, the cybersecurity-based regulations discussed here impose costs and restrictions on a firm's operations. One aspect of the property rights inspection relates to the Fifth Amendment claim of 'regulatory taking.' Establishing whether regulation of public utilities constitutes a Fifth Amendment 'regulatory taking'[231] requires a case-by-case analysis to account for: (1) its economic impact; (2) its interference with investment-backed expectations, and (3) the nature of government actions.[232] In addition, the regulation must be precise; vague regulation could be considered unconstitutional.[233] However, reasonable and narrowly tailored regulations usually pass constitutional muster. The regulation can also be challenged for restricting occupational rights. However, these rights (especially in this specific context) are most likely not constitutionally protected, and therefore this challenge will not prove substantial.[234]

An even more substantial rights-based challenge pertains to the *right to privacy* and fears of its violation.[235] As opposed to the previous discussion, which focused on the relevant rights of the CI operators, the discussion on privacy rights focus on the rights of the vast customer base. Indeed, CI firms hold colossal amounts of consumer personal data. Consider telecom operators, with their massive datasets of metadata regarding phone calls, data exchanges, and locations, as well

230. While there is no 'freedom of occupation right' under the U.S. Constitution, "enactments affecting occupation . . . must . . . not . . . violate due process as required by the Fifth Amendment in the case of Federal legislation and of the Fourteenth Amendment in the case of State legislation." Fraley N. Weidner, *Freedom of Occupation*, 25 MARQ. L. REV. 8, 8 (1940).

231. U.S. CONST. amend. V.

232. *See* Penn Cent. Transp. Co. v. New York City, 438 U.S. 104, 124 (1978). For a review of existing cases regarding this matter, see ROBERT MELTZ, CONG. RESEARCH SERV., 97-122, TAKING DECISIONS OF THE U.S. SUPREME COURT: A CHRONOLOGY (2015), https://fas.org/sgp/crs/misc/97-122.pdf [https://perma.cc/KVZ9-XYDW].

233. *See, e.g.*, Grayned v. City of Rockford, 408 U.S. 104, 108 (1972) ("It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined."). However, the lack of precision is not itself offensive to the requirements of due process. *See* Roth v. United States, 354 U.S. 476, 491 (1957) (" '[T]he Constitution does not require impossible standards'; all that is required is that the language 'conveys sufficiently definite warning as to the proscribed conduct when measured by common understanding and practices . . . .' " (quoting United States v. Petrillo, 332 U.S. 1, 7-8 (1947))).

234. *See supra* note 230 and accompanying text.

235. For a discussion of possible privacy violations in this context, see Kesan & Hayes, *supra* note 33, at 1549-54.

as their access to the content of the communications themselves. Beyond telecommunications, in the age of 'smart metering,'[236] energy providers can map out entire lives using the data at their disposal.

As a general outline of privacy risks,[237] we note concerns related to the two distinct objectives of government—data sharing (including real-time data) and enforcement of appropriate technical standards. Each of these raises distinct privacy concerns. First, consider data sharing. As explained above, the government will aggregate and store massive amounts of data pertaining to the CI's ongoing operation to limit information failures.[238] While the government may not intend for the data to be personal, some could prove to be personally identifiable, i.e., it may be possible to match specific individuals using data analytics relying on additional and external data sets.[239] This is true because the data pertains to traffic and usage of the networks, and therefore possibly reflects the traits and preferences of its users. In this instance, privacy interests are compromised as personal information makes its way to the government without consumers' specific approval. This in itself could cause security risks as well: a central database of such sensitive nature encourages hacking attempts, particularly if the data is unsecure.

Second, consider enforcing technical standards. At this point, the government is faced with a difficult decision. Lenient enforcement of such standards—which might be reduced to providing requirements and reviewing response reports—will have limited implications on consumer privacy rights; yet it risks being proved ineffective. A more extensive monitoring model allows for constant monitoring and authorization to engage in surprise inspections and audits to ensure a higher level of compliance. But such extensive inspections of CI systems could compromise user rights; again, their personal data could be subject to government scrutiny as part of these monitoring initiatives. Even if,

---

236. *See* Federico Guerrini, *Smart Meters: Between Economic Benefits and Privacy Concerns*, FORBES (June 1, 2014, 1:15 PM), http://www.forbes.com/sites/federicoguerrini/2014/06/01/smart-meters-friends-or-foes-between-economic-benefits-and-privacy-concerns/#73f03f1151a9 [https://perma.cc/Z3U3-7V5Y]. For a discussion of meeting the privacy concerns of smart metering in Britain, see Ian Brown, *Britain's Smart Meter Programme: A Case Study in Privacy by Design*, 28 INT'L REV. L. COMPUTERS & TECH. 172 (2014).

237. For more on the privacy concerns raised by this issue, see generally Bambauer, *Sharing Shortcomings*, *supra* note 158.

238. *Id.* at 484 ("Current information-sharing approaches thus create risks to privacy, by accumulating a storehouse of sensitive personal information . . . .").

239. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1748 (2010).

in practice, government agents did not actually review this information, their ability to do so is troubling enough.[240] Such worries go beyond other instances in which government officials often engage in inspections, such as those pertaining to food and drug manufacturing or enforcing building standards and fire codes. In all these instances, government officials (merely) enter and inspect private property. The cyber context, however, features a personal-data rich environment in which the potential for privacy harm is substantially enhanced.

Both of the noted scenarios compromise privacy interests by subjecting individuals to the threatening surveillance capabilities of the State. They might also have a chilling effect, where individuals may actually curb or reconsider specific forms of behavior in light of the threat of government access to personal data. Therefore, structuring a regulatory scheme that provides government with access to personal information held by CI operators compromises privacy rights on a normative and theoretical level. The problems arising here also exceed those unfolding in instances in which the firms share the information voluntarily with the government; in these instances, information sharing would likely be limited and subject to provisions of the consumer contracts.

It is unclear whether rules requiring data sharing by and technical auditing of CIs raise actual constitutional concerns under the current doctrine. The privacy rights here discussed are impermissibly compromised when the individual's reasonable expectation of privacy is breached.[241] This usually requires an illegal or unauthorized search[242] to occur. It is currently unclear whether individuals have a reasonable expectation of personal information privacy regarding personal information (especially metadata) held by 'third parties' such as public utilities.[243] Nonetheless, privacy concerns regarding both the potential accessibility to personal data, as well as actual access to such data, must

---

240. *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, *supra* note 11, at vii ("The Federal Government recognizes the risk that technologies designed to protect information and systems, if not carefully utilized, could inadvertently undermine civil liberties. Even with the best of intentions, technology that protects against intrusions, when cast too broadly, might profile innocent activity. Where individual rights are at issue, careful consideration of all related issues is essential.").

241. The Fourth Amendment grants a right for people "to be secure in their persons, houses, papers, and effects, [and] against unreasonable searches and seizures." U.S. CONST. amend. IV.

242. Blake Covington Norvell, *The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation?*, 11 YALE J.L. & TECH. 228, 233 (2009) ("In approaching a question of whether the Fourth Amendment has been violated, one must first determine if a 'search,' conducted by or on behalf of the government, has taken place.").

243. The general notion is that such right does not exist. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979). However, this understanding is under attack. *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring). For different discussions of this issue in the context of the Snowden revelations regarding the NSA's surveillance projects, see Klayman v. Obama, 957 F. Supp. 2d 1, 10-11 (D.D.C. 2013). In addition, see United States

be considered. Notably, the current constitutional balance as set by the Supreme Court might be realigned. Moreover, in light of public pressure, the legislature may consider a more protective standard of privacy (which goes beyond the limited protection afforded by the Constitution) when considering the regulation of this matter, as it recently did in related contexts of national security and law enforcement.[244]

Privacy-based concerns do not necessarily undermine the notion that government must closely regulate CI cyber security efforts. Rather, they should be considered when designing a regulatory scheme. For instance, they should impact the form of information shared and the manner in which government audits are conducted. Information sharing (either voluntarily or under mandate) or government access to CI datasets, must only be permitted after the implementation of oversight and safeguard mechanisms that protect privacy objectives.

To conclude, our analysis points to some weaker rights of the firm that might be compromised by such regulation, and a substantial right—consumer right of privacy—the infringement of which must be considered in any regulation designed. A concluding note regarding this matter pertains to the general notion of *legality* and the fear of overall inappropriate government intervention. The legal and technological mechanisms discussed here open the door to governmental overreach.[245] They evoke fear of the creeping extension of state power and thus undermining the rule of law. This overall concern must be accounted for as well when designing the relevant regulatory scheme, and is closely tied to the notion of the secrecy the process entails, which we now address.

4. Secrecy

A regulatory scheme governing CI cybersecurity will most likely be premised upon a certain degree of secrecy, given the nature of government activities in this context, as well as government's overall preference for opacity.[246] As with our previous discussion concerning privacy,

---

v. Davis, 785 F.3d 498, 512–14 (11th Cir. 2015) (en banc) (rejecting the notion that the "third-party doctrine" has been limited by *Jones*).

244. Jedidiah Bracy, *In Post 9/11 Reversal, U.S. Enacts Surveillance Reform*, THE PRIVACY ADVISOR (June 3, 2015), https://iapp.org/news/a/in-post-911-reversal-u-s-enacts-surveillance-reform [https://perma.cc/27CA-YA6Y]. This change was premised on the following committee's recommendation: THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES., LIBERTY AND SECURITY IN A CHANGING WORLD 79-85, 89-121 (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/34TG-3YZK].

245. KERFOOT, *supra* note 138, at 7.

246. Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 890 (2006) ("[G]overnment seems eternally resistant to disclosure.").

the notion of 'secrecy' does not constitute a definite critique of the government-based regulatory scheme, yet is merely a factor that must be considered in its design.

The extent of secrecy needed is also linked to decisions regarding the *nature* of the government entity that oversees this form of cybersecurity regulation. In the United States, much of the current authority is vested in the DHS—which is not part of the military or intelligence community. The DHS's civilian culture is reflected in its transparency practices regarding CIP regulation.[247] On its website, anyone can read recommended security standards and guidelines, all openly published. Questionnaires sent to CI operators on the subject are also available as well.[248]

Yet one can easily imagine an alternative structure, one in which an intelligence agency, such as the NSA, is vested with this authority.[249] Worldwide, countries are struggling with determining which type of entity should be vested with this authority.[250] Transferring the authority discussed herein to a security/intelligence/military-like entity could have various operational benefits. Such a scheme would allow for better integration of information from intelligence sources, combining the mission of protecting civilian CIs with military purposes such as prevention and even preemptive attacks. One could even envision a situation in which the government agency withholds information on a vulnerability found while monitoring cyber defenses from CIs and the public, opting to use it offensively. Note, however, that the balance between CI sustainability and national security, which unfolded in this last example regarding the discovery of vulnerabilities,

---

247. *See* Michelle Richardson, *Keep Domestic Cybersecurity Efforts in Civilian Hands*, ACLU (Apr. 27, 2012, 8:37 AM), https://www.aclu.org/blog/keep-domestic-cybersecurity-efforts-civilian-hands [https://perma.cc/FS85-YQ3B].

248. *See* DEP'T OF HOMELAND SEC., RISK-BASED PERFORMANCE STANDARDS GUIDANCE: CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (2009), https://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf [https://perma.cc/EPF9-A8VB]; DEP'T OF HOMELAND SEC., CSAT SECURITY VULNERABILITY ASSESSMENT APPLICATION: INSTRUCTIONS (2011), https://www.dhs.gov/sites/default/files/publications/csat_sva-instructions_508.pdf [https://perma.cc/NF49-PE8Y].

249. ROSENZWEIG, *supra* note 138, at 197; Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 119, 136 (2010) (warning against empowering the NSA, due to its secrecy).

250. In Germany, the recently enacted IT Security Act (ITSG) vests the authority of regulating and approving cyber security standards with the "Federal Office for Information Security" (BSI). This authority is *not* part of the German intelligence service. *See* Gabel & Schuba, *supra* note 130. In Israel, this issue is currently in flux, as the authority regarding cyber security of CI is being shifted from the security and intelligence authorities to designated cyber authorities. *See* Barak Ravid, *Israeli Security Agencies in Turf Battle Over Cyber War; Netanyahu to Decide*, HAARETZ (Sept. 14, 2014, 2:10 AM), http://www.haaretz.com/israel-news/1.615637 [https://perma.cc/DW58-G9R3]; sources cited *supra* note 135.

might not be publicly acceptable. Some might not even see this outcome as a 'benefit' at all. Nonetheless, such a shift in the task of regulating CI protection to an intelligence or military agency offers a very different management culture. This would obviously have an impact on the extent of secrecy and transparency of the regulatory process.[251]

It is therefore imperative to examine the importance of secrecy (or transparency) in the cyber risk regulation scheme as either a primary objective or an unavoidable byproduct of a specific regulatory strategy. Intuitively, secrecy can ensure a high level of cybersecurity. This intuition is premised on the conventional wisdom that revealing information to the public, and thus to the enemy, may harm security objectives. 'Loose lips sink ships,' the well-known World War II phrase, clearly expresses this notion. Therefore, secrecy is certainly not an unfortunate consequence, but a coveted objective.

But secrecy in the context of cybersecurity is distinct from that of military secrecy: Transparency does not pose a threat like those posed by leaked secure information; for example, the location of ships at battle.[252] The potential attacker most likely knows the defensive measures deployed or could acquire this knowledge.[253] Therefore, transparency does not necessarily increase risks and has many advantages. For instance, transparency could actually promote better cyber protection. Informing the public of the selected cyber security methods and strategies allows control and oversight of the agency and CI operators and consequentially motivates firms to improve and increase their protection levels.[254]

In contrast, secrecy could attract criticism and thus erode public trust. The lack of trust can directly undermine the success of cyber protection efforts. Public criticism of a secretive cyber protection scheme could adversely affect a variety of players in the field. Politicians, who fear negative public image could weaken the scheme or fail to promote it; the press, due to criticism, might strive to undermine it; and even private firms providing infrastructure or defensive measures may choose to not cooperate with the state in this regard, even when

---

251. *See* ROSENZWEIG, *supra* note 138, at 227.

252. *See* Benkler, *supra* note 207, at 294-95; KAREN SCARFONE ET AL., GUIDE TO GENERAL SERVER SECURITY: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2-4 to 2-5 (2008), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf [https://perma.cc/M54M-ML9E] (listing general information security principles); *see generally* Jerome H. Saltzer & Michael D. Schroeder, *The Protection of Information in Computer Systems*, 63 PROC. INST. ELECTRICAL & ELECTRONIC ENGINEERS 1278 (1975) (exploring the mechanics of protecting computer-stored information from unauthorized use).

253. *See* Swire, *supra* note 206, at 194.

254. *See, e.g.*, Benkler, *supra* note 207, at 284 ("Secrecy insulates self-reinforcing internal organizational dynamics from external correction.").

required by law. This, indeed, could be the reason the NSA is *not* fully engaged in cyber-related activities in the United States, although it certainly has the capacity to do so.[255]

Finally, greater transparency can mitigate several concerns linked to the potential rights violations noted above. Secrecy essentially increases the power of policymakers, which increases the public's fears and the actual risk that policymakers will exceed their mandate and undermine legality. Transparency reduces this fear. In addition, transparency aids in safeguarding other fundamental rights, particularly the right to privacy, mainly by ensuring a legal and public discourse on the issue, which will enable audit mechanisms and improve citizen protections. In addition, public insight into government actions is a right on its own, although it is often balanced with other rights.[256]

To conclude, we return to the notion of design. Our objective in this Section is not to advocate for full and complete transparency of all actions of governmental groups regulating cyber security. However, it does call for a middle ground—e.g., publishing general principles as to how the CIs are regulated and inspected (a practice the DHS currently follows)—which allows for partial fulfillment of transparency goals. Another option is requiring that the relevant regulating entity selectively share its information while collaborating with external experts (of both technological and social background). This Section also provides various factors to consider when deciding on the nature of the agency vested with the governmental authorities discussed herein, as well as the extent of their operations.

5. Centralization

A CIP government-based regulatory scheme may feature *centralization*—the concentration of all cyber-related protection schemes within one expert entity. Prima facie centralization is seemingly advantageous in this regulatory strategy, as is explained above.[257] However, centralization has its own shortcomings. Yet again, we must note that the centralization issue is not an inherent flaw in a government regulatory scheme, but an element to be considered in its design.

Centralization of decisions could compromise the principle of *diversity*,[258] an important concept often noted in security-related literature.

---

255. *See* ROSENZWEIG, *supra* note 138, at 197.

256. Tal Z. Zarsky, *Transparent Predictions*, U. ILL. L. REV. 1503, 1530-31 (2013); Fenster, *supra* note 246, at 895-96.

257. *See supra* Section V.A.

258. *See* ROSENZWEIG, *supra* note 138, at 180; Benkler, *supra* note 207, at 295; Julie Gallagher, *Importance of Redundancy, Diverse Systems Grows Post-9/11, Stresses Hartford*

This concept states that CI operators must refrain from implementing the same or similar cybersecurity measures in a variety of CI contexts. Heterogeneity is therefore crucial to assure cybersecurity, so that a weakness in one security system will not necessarily affect other systems.[259] With diverse systems in place, damage caused by a successful cyber attack that relied on an identified vulnerability will be specific, easy to confine, and simpler to fix.

However, it would be unwise to conclude that centralized cyber regulation leads to homogeneity in cybersecurity measures. We need not assume that the centralized entity is unaware of the problems of homogeneity and will not implement heterogeneous models of protection. On the contrary, arguably centralized cyber regulation can optimally *ensure* diversity. Given their central position, this entity can indeed assure that different cybersecurity measures are applied at different junctures, and thus, help increase the resilience of the system as a whole.

Nonetheless, centralization can pose risks to the diversity principle. The regulating entity is, by nature, led by a single management philosophy and approach. This fact could lead to unified defense mechanisms for the country's infrastructure, and inherently risk the state. In light of this concern, the alternative model of CI owners' self-regulation may offer an advantage in that it may encourage conceptual diversity.[260] Indeed, when the central entity takes merely an advisory role, this concern is mitigated. Another solution is sectorial regulation. However, this last solution raises many problems that result from power struggles as to the confines of every sector and the authority to regulate entities that might fall within several sectors.

VI. THE OPTIMAL CIP MODEL: A BLUEPRINT

We now turn from our analytical study and roadmap of policy critiques to concrete recommendations. We must first acknowledge that each context calls for a separate balance and analysis; nonetheless, our discussion above allows us to point out several crucial elements for optimal CI protection, even though they will no doubt entail a few disadvantages.

We begin with several general observations that are undisputed: the fear of cyber attacks is not a work of fiction. CIs will very likely be attacked through cyber means, and these attacks will most likely

---

Financial's Lowenthal, INFORMATIONWEEK: INS. & TECH. (Oct. 24, 2001, 9:05 AM), http://www.insurancetech.com/architecture-infrastructure/14706497 [https://perma.cc/9CDA-LVCQ].

259. *See* Nojeim, *supra* note 149, at 130 (arguing that setting a single standard "could actually worsen security because a vulnerability in a standardized system could affect many entities").

260. Coldebella & White, *supra* note 215, at 241 ("A centrally planned, one-size-fits-all regulatory scheme would almost certainly eliminate useful, industry-developed security measures and replace them with an ill-fitting, nondynamic slate of requirements.").

cause substantial damage.[261] Accordingly, it is undisputable that CIs require proactive protection from cyber attacks. As we show, a market-based approach, which has many advantages, cannot provide adequate protection on its own. Providing mere ex post incentives are also insufficient. Therefore, the current U.S. CIP approach is misguided and should be thoroughly reexamined. Our discussion in Part III leads to the conclusion that the state must play a more substantial role in CIP. In addition, and in interests of efficiency, expertise, and simplicity, a centralized agency is fitting for this role.[262] Yet such a substantial role could take many forms. In the next few paragraphs we explore several central options

Designing an optimal CIP model requires paying special attention to the three central failings of the market-based approach: *inadequate information sharing*, *lack of knowledge transfers*, and *underinvestment*.[263] Let us examine their implications separately. *Information sharing* is an important (yet on its own, insufficient) [264] factor in cybersecurity schemes. It is essential for the identification of vulnerabilities that need patching and the early interception of threats.[265] It allows CI operators to pool resources and enables collaborative problem solving.[266]

Therefore, the state must continue to proactively promote this form of data exchange among parties in real time. The government's role is to facilitate—by structuring platforms, granting immunity for the practices of data transfers (from possible liability for privacy violations or antitrust wrongs), and assuring a high level of security in the process. If these steps prove insufficient, the state may even be required to further mandate data sharing among the CIs themselves. Yet given privacy-related risks, it need not maintain a dataset of its own, unless such a data aggregation process was subjected to specific (perhaps

---

261. One example of a successful cyber-attack on a power grid occurred in December 2015, in Ukraine, and interrupted power for 225,000 Ukrainians. *See* Tami Abdollah, *US: Sophisticated Attackers Hacked Ukrainian Electric Grid*, YAHOO (Feb. 26, 2016), https://www.yahoo.com/tech/us-sophisticated-attackers-hacked-ukrainian-electric-grid-212811154--finance.html [https://perma.cc/Q4P8-UPFN].

262. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 208, at 15.

263. *See supra* Part IV.A.

264. *See, e.g.*, Clayton, *supra* note 107 ("[E]xperts say cybersecurity needs go far beyond information sharing.").

265. Palmer, *supra* note 17, at 314-16 (describing the need for public-private information sharing in CIP); Tim Molino, *Sharing Cyber Threat Information: How It Would Work, and Why It Would Help Bolster Security*, BSA 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 [https://perma.cc/5XM7-K6D4].

266. *See* Palmer, *supra* note 17, at 348.

even judicial) review.[267] The fact that personal information is held by private entities does not mean that customers will approve of the data commonly winding up in the hands of the government.

Attending to and promoting sufficient *knowledge transfers* is no less challenging. While the knowledge gap problems noted are substantial, they do not necessitate extensive governmental intervention, nor do they mean that only the government can set appropriate cyber standards. Rather, the knowledge gap could be closed by facilitating knowledge sharing and transfer among relevant parties. This, in fact, is government's proper role—assuring that cyber companies, CI operators, and government agencies join together in round tables to exchange and share knowledge. The state too must have a seat at the table; however, this does not imply that it should run the exchange or control the outcome. Furthermore, the state should not have the ability to dictate the standard eventually adopted, but rather provide feedback and contribute expertise and experience.[268]

Finally, we approach the regulator's most substantial challenge—the fear of *underinvestment in CI cybersecurity measures*. Here it is important to distinguish between the various facets related to this concern. Generally, to overcome the 'underinvestment' challenge, a technological standard must be formulated, chosen, assigned, monitored, and enforced.

Given our analysis of knowledge sharing, the government does not need to formulate the standard for CI cyber-protection. It should, however, select one or more standards as a minimal threshold by which the CIs *must* abide. A panel of third-party representatives should examine these selections to ensure that the forms of undue influence noted above did not play a major role in the government's decisions. In addition, such a review process is important to assure that other governmental incentives, such as intentionally weakening security measures to enable surveillance,[269] do not play a dominant role in the standard setting process. It is also important to structure the process

267. Congress should explicitly define what constitutes "relevant information" for these purposes; otherwise, it would enable warrantless information-sharing on anything, regardless of cybersecurity. We witnessed such vagueness in the formation of "cyber threat indicators" under the Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242. *See supra* Section III.A.1.

268. For proposals as to how such standards should be set, see Kesan & Hayes, *supra* note 33, at 1556-58.

269. The U.S. government has most likely engaged in such practices in the past. News reports and expert studies indicate that the NSA influenced NIST to introduce a weakness into an encryption standard so to allow future code-breaking and surveillance. *See* Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=1 [https://perma.cc/WM4M-BD7C].

in a manner that maintains the involvement of the CIs themselves. Such involvement is important to avoid a 'box checking' compliance culture[270] and to assure that CIs maintain their willingness and ability to quickly respond to changing threats. This could be achieved by allowing firms to challenge the standard chosen and offer more appropriate and efficient measures.

The state must act to monitor implementation of these requirements and cannot rely upon ex post regulation or other incentive structures. It must do so by setting reporting requirements to ensure compliance with the noted standards. In this sense, the United States could follow the lead of the European Union in their enacting of recent regulation.[271] In addition, the government must play a more substantial role in enforcing the standards selected. However, if and when monitoring and auditing enforcement entails compromising privacy rights, such tasks must be allocated to private parties (which will report to the authorities). This step will mitigate public concerns of unchecked access to personal data by government officials. Finally, the state must be willing and able to sanction, and not just shame, noncompliant CIs. Carrying out these steps on a large, national scale would prove costly; yet, such costs are necessary in the current state of affairs.

Obviously, every regulatory scheme calls for exceptions, as is the case with the power and chemical sector. Here too, we suggest the United States follow the EU's lead and introduce enhanced regulations for the telecommunications sector as it serves a double function in this context. Telecommunications are vulnerable to cyber attacks on their own and can also be used to launch cyber attacks against other CIs. Thus, attacks against this sector have particular ramifications. The United States has recognized this threat, and version 3.0 of its 'Einstein' project (a U.S.-CERT program) is designed to prevent attacks by monitoring government computer traffic on private sector sites.[272] Thus, the telecom sector must be singled out and requires greater, more stringent mandatory CIP standards, although perhaps not standards as aggressive as those employed in the controversial 'Einstein' project.[273] But this type of intervention should be an exception to

270. *See supra* Section V.B.1.

271. *See supra* Section III.B.

272. *See Homeland Security Seeks Cyber Counterattack System*, CNN (Oct. 4, 2008), http://edition.cnn.com/2008/TECH/10/04/chertoff.cyber.security/ [https://perma.cc/8UTU-7MPT].

273. For a critique of this initiative, see Steven M. Bellovin et al., *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure*, 3 HARV. NAT'L SECURITY J. 1 (2011).

the general CIP strategies and premised on a relevant risk assessment.[274] Furthermore, such steps must be implemented only after safeguards to assure sufficient protections for privacy are applied.

Lastly, we turn to the complicated issue of institutional designation and design. Given the value of transparency and the risks to individual rights, CI cyber regulation should be carried out by entities outside the military/intelligence community as much as possible. In specific contexts, where operational demands require regulation by the military/intelligence arm, greater secrecy could be tolerated. In addition, and in the interest of protecting rights, promoting efficiency, and ensuring heterogeneity in protection strategies, third parties and external experts should be consulted when possible. Furthermore, various forms of oversight by other governmental branches should be introduced when transparency must be limited for security reasons.

VII. CONCLUSION

It is undisputable that CIs require protection—even the term chosen indicates their 'critical' nature. It is also evident that the cyber age and other geo-political risks have changed the scope of threats to CIs worldwide. Addressing the issue at hand raises several complicated questions. While it is relatively simple to explain 'why' CIs require protection and 'why' the type of protection offered must be reassessed, it is far more complicated to determine 'which' CIs should be regulated and 'how' that might be done.

This Article responds to these questions, analyzes the benefits and shortcomings of potential CIP regulation, and draws from the international effort to respond to this threat and the existing scholarship addressing these efforts. Our discussion leads us to recommend greater government involvement through a central authority—one that must be carefully tailored to preserve individual rights that could be compromised. This Article calls for recalibrating some of the existing regulatory structure as soon as possible, recognizing that danger of upcoming attacks is imminent.

Beyond our analysis herein, it is important to note that in protecting CIs, no one nation is an island. Infrastructures are generally interconnected. Attacks against one could impact another country and its citizens. Therefore, the international aspects of this discussion must be recognized. Global information and knowledge sharing, as well as strategies to ensure compliance with internationally-set standards are becoming crucial for any CIP model. Obviously, implementing such

274. For more on the process of risk assessment in CIP, see Yacov Haimes et al., *Risk Analysis in Interdependent Infrastructures*, *in* CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 19, at 297; Marcelo Masera & Igor Nai Fovino, *A Service-Oriented Approach for Assessing Infrastructure Security*, *in* CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 19, at 367.

schemes will prove to be a difficult and delicate task and information sharing requirements must constantly be balanced against various state interests in the global realm. This additional analysis requires further research, which must follow.