REGULATING CYBER-SECURITY

Nathan A. Sales,
George Mason University School of Law

***Northwestern University Law Review*,**
Vol. 107, No. 4, pp. 1503-1568, 2013

George Mason University Law and Economics Research Paper Series

12-35

Printed in U.S.A.
Northwestern University Law Review
Vol. 107, No. 4

Articles

REGULATING CYBER-SECURITY

Nathan Alexander Sales

ABSTRACT—The conventional wisdom is that this country's privately owned critical infrastructure—banks, telecommunications networks, the power grid, and so on—is vulnerable to catastrophic cyber-attacks. The existing academic literature does not adequately grapple with this problem, however, because it conceives of cyber-security in unduly narrow terms: most scholars understand cyber-attacks as a problem of either the criminal law or the law of armed conflict. Cyber-security scholarship need not run in such established channels. This Article argues that, rather than thinking of private companies merely as potential victims of cyber-crimes or as possible targets in cyber-conflicts, we should think of them in administrative law terms. Many firms that operate critical infrastructure tend to underinvest in cyber-defense because of problems associated with negative externalities, positive externalities, free riding, and public goods—the same sorts of challenges the modern administrative state faces in fields like environmental law, antitrust law, products liability law, and public health law. These disciplines do not just yield a richer analytical framework for thinking about cyber-security; they also expand the range of possible responses. Understanding the problem in regulatory terms allows us to adapt various regulatory solutions—such as monitoring and surveillance to detect malicious code, hardening vulnerable targets, and building resilient and recoverable systems—for the cyber-security context. In short, an entirely new conceptual approach to cyber-security is needed.

AUTHOR—Assistant Professor of Law, George Mason University School of Law. Thanks to Jonathan Adler, Stewart Baker, Derek Bambauer, Bobby Chesney, Eric Claeys, Tim Clancy, Orin Kerr, Michael Krauss, Deirdre Mulligan, Steve Prior, Jeremy Rabkin, Paul Rosenzweig, J.W. Verret, Ben Wittes, and Todd Zywicki for their helpful comments. I'm also grateful to participants in workshops at Syracuse University College of Law and the Republic of Georgia's Ministry of Justice. Special thanks to the Center for Infrastructure Protection and Homeland Security for generous financial support.

INTRODUCTION

The Red Army had been gone for years, but it still had the power to inspire controversy—and destruction.[1] In April 2007, the government of Estonia announced plans to relocate a contentious Soviet-era memorial in its capital city of Tallinn. Known as the Bronze Soldier, the Soviets erected the statue in 1947 to commemorate their sacrifices in the Great Patriotic War and their "liberation" of their Baltic neighbors. The local population, which suffered under the Bolshevik boot for decades, understandably saw the monument in a rather different light. Not long after the announcement, the tiny nation was hit with a massive cyber-attack. Estonia, sometimes nicknamed "E-stonia," is one of the most networked countries in the world—its citizens bank, vote, and pay taxes online[2]—and it ground to a halt for weeks. The country's largest bank was paralyzed. Credit card companies took their systems down to keep them from being attacked. The telephone network went dark. Newspapers and television stations were knocked offline. Who was responsible for launching what has come to be

[1] The events in this paragraph are described in JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 127–30 (2011); RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 11–16 (2010); and Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (London), May 17, 2007, at 1.

[2] Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 61 & n.14 (2010).

known as Web War I?[3] The smart money is on Russia, though no one can say for sure.

It could happen here. Government officials like Richard Clarke, the former White House cyber-security czar, have been warning of "an electronic Pearl Harbor" for years.[4] Others lament the "gaping vulnerabilit[ies]"[5] in America's cyber-defenses and speculate that the economic effect of a major assault could be "an order of magnitude" greater than the September 11, 2001 terrorist attacks.[6] Academic commentators generally agree. Some see the danger as "monumental"[7] and the country's "most pervasive and pernicious threat."[8] Others predict that America's failure to secure its cyber-assets "could take down the nation's entire security and economic infrastructure"[9] and "bring this country to its knees."[10] It has even been suggested that "[t]he very future of the Republic" depends on "protect[ing] ourselves from enemies armed with cyber weapons."[11] There are some naysayers,[12] but the consensus that we stand on the brink of a cyber-calamity is both broad and deep.

---

[3] *War in the Fifth Domain*, ECONOMIST, July 3–9, 2010, at 25, 28; *see also* CLARKE & KNAKE, *supra* note 1, at 30; David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 799 (2012).

[4] Richard Clarke, *Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks*, 12 DEPAUL BUS. L.J. 33, 38 (1999–2000).

[5] Joby Warrick & Walter Pincus, *Senate Legislation Would Federalize Cybersecurity; Rules for Private Networks Also Proposed*, WASH. POST, Apr. 1, 2009, at A4.

[6] Max Fisher, *Fmr. Intelligence Director: New Cyberattack May Be Worse than 9/11*, ATLANTIC (Sept. 30, 2010, 2:28 PM), http://www.theatlantic.com/politics/archive/2010/09/fmr-intelligence-director-new-ttack-may-be-worse-than-9-11/63849/ (quoting former Director of National Intelligence Mike McConnell); *see also* EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW 1 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies.").

[7] William C. Banks & Elizabeth Rindskopf Parker, *Introduction*, 4 J. NAT'L SEC. L. & POL'Y 7, 11 (2010).

[8] Walter Gary Sharp, Sr., *The Past, Present, and Future of Cybersecurity*, 4 J. NAT'L SEC. L. & POL'Y 13, 13 (2010); *see also* CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 11 (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf; Greg Rattray et al., *American Security in the Cyber Commons*, *in* CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD 137, 145 (Abraham M. Denmark & James Mulvenon eds., 2010).

[9] Opderbeck, *supra* note 3, at 798.

[10] Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1020 n.45 (2001) (quoting Chris O'Malley, *Information Warriors of the 609th*, POPULAR SCI., July 1997, at 71, 72).

[11] Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SEC. L. & POL'Y 155, 156 (2010).

[12] *See, e.g.*, Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 604 (2011); Charles J. Dunlap, Jr., *Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy*, 76 INT'L L. STUD. 353, 361 (2002); Seymour M. Hersh, *The Online Threat*, NEW YORKER, Nov. 1, 2010, at 44, 48; Martin Libicki, *Rethinking War: The Mouse's New Roar?*, FOREIGN POL'Y, Winter 1999–2000, at 30, 38; Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat*

A large-scale cyber-attack on this country, as in Estonia, likely would target privately held critical infrastructure—banks, telecommunications carriers, power companies, and other firms whose compromise would cause widespread harm.[13] Indeed, America's critical infrastructure, approximately 85% of which is owned by private firms,[14] already faces constant intrusions.[15] Yet the private sector's defenses are widely regarded as inadequate. Companies are essentially on their own when it comes to protecting their computer systems, with the government neither imposing security requirements nor bearing a share of the resulting costs.[16] According to Bruce Smith, the United States follows a "bifurcated approach to network security" that "relie[s] predominantly on private investment in prevention and public investment in prosecution."[17] Christopher Coyne and Peter Leeson likewise stress that our defensive strategy "is simply the sum of dispersed decisions of individual users and businesses."[18] Regular firms that operate in competitive markets (such as online retailers) may be

Inflation in Cybersecurity Policy 6–7 (Mercatus Ctr. at George Mason Univ., Working Paper No. 11-24, 2011), *available at* http://mercatus.org/sites/default/files/WP1124_Loving_cyber-_bomb.pdf.

[13] *See* CLARKE & KNAKE, *supra* note 1, at xiii; Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 182 (2006). Federal law defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (2006). Some types of critical infrastructure are more important, and less likely to be adequately defended, than others.

[14] Todd A. Brown, *Legal Propriety of Protecting Defense Industrial Base Information Infrastructure*, 64 A.F. L. REV. 211, 220 (2009); Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SEC. L. & POL'Y 233, 240 (2010); Christopher J. Coyne & Peter T. Leeson, *Who's to Protect Cyberspace?*, 1 J.L. ECON. & POL'Y 473, 476 (2005); Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SEC. L. & POL'Y 119, 135 (2010); Benjamin Powell, *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry*, 1 J.L. ECON. & POL'Y 497, 497 (2005); Paul Rosenzweig, *Cybersecurity and Public Goods: The Public/Private "Partnership,"* HOOVER INST. 2 (2011), http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf, *reprinted in* PAUL ROSENZWEIG, CYBERWARFARE: HOW CONFLICTS IN CYBERSPACE ARE CHALLENGING AMERICA AND CHANGING THE WORLD 156–75 (2012).

[15] *See* MCAFEE & CTR. FOR STRATEGIC & INT'L STUDIES, IN THE DARK: CRUCIAL INDUSTRIES CONFRONT CYBERATTACKS 6 (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf; Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1537 (2010); Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261, 2263 (2003); Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 201, 205 (2006).

[16] *See* Yasuhide Yamada et al., *A Comparative Study of the Information Security Policies of Japan and the United States*, 4 J. NAT'L SEC. L. & POL'Y 217, 219–20 (2010).

[17] Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 173 (2005).

[18] Coyne & Leeson, *supra* note 14, at 475–76; *accord* AM. BAR ASS'N, NATIONAL SECURITY THREATS IN CYBERSPACE 8 (2009), *available at* http://nationalstrategy.com/Portals/0/National%20Security%20Threats%20in%20Cyberspace%20%20FINAL%2009-15-09.pdf; Banks & Parker, *supra* note 7; Nojeim, *supra* note 14, at 121.

adequately protecting their systems against ordinary intruders (such as recreational hackers). But strategically significant firms in uncompetitive markets (such as power companies and other public utilities) seem less likely to maintain defenses capable of protecting their systems against skilled and determined adversaries (such as foreign intelligence services).

The poor state of America's cyber-defenses is partly due to the fact that the analytical framework used to understand the problem is incomplete. The law and policy of cyber-security are undertheorized. Virtually all legal scholarship approaches cyber-security from the standpoint of the criminal law or the law of armed conflict.[19] Given these analytical commitments, it is inevitable that academics and lawmakers will tend to favor law enforcement and military solutions to cyber-security problems. These are important perspectives, but cyber-security scholarship need not run in such narrow channels. An entirely new approach is needed. Rather than conceiving of private firms merely as possible victims of cyber-crimes, or as potential targets in cyber-conflicts, we should think of them in regulatory terms.[20] Many companies that operate critical infrastructure tend to underinvest in cyber-defense because of negative externalities, positive externalities, free riding, and public goods

[19] Bambauer, *Conundrum*, *supra* note 12, at 588–89. For examples of the criminal law approach, see Banks & Parker, *supra* note 7, at 9; Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 190–97 (2000); Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 407–08 (2007); Katyal, *Criminal Law*, *supra* note 10, at 1013–38; Katyal, *Digital Architecture*, *supra* note 15, at 2263–88; Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 241–52 (2000); Opderbeck, *supra* note 3, at 822–26; and Yang & Hoffstadt, *supra* note 15, at 201–07. For examples of the armed conflict approach, see Brown, *supra* note 13, at 182–90; Condron, *supra*, at 408; David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 90–100 (2010); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 214–29 (2002); Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 70–82 (2010); William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97, 101–05 (2010); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 900–24 (1999); Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 6–10 (2009); and Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 426–37 (2011). There are exceptions. Some scholars understand cyber-security in public health terms. *See* IBM, MEETING THE CYBERSECURITY CHALLENGE: EMPOWERING STAKEHOLDERS AND ENSURING COORDINATION 11–14 (2010), *available at* http://www-304.ibm.com/easyaccess3/fileserve?contentid=192188; Jeffrey Hunker, *U.S. International Policy for Cybersecurity: Five Issues that Won't Go Away*, 4 J. NAT'L SEC. L. & POL'Y 197, 202–04 (2010); Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 DAEDALUS 70, 77–88 (2011); Rattray et al., *supra* note 8, at 151–66. Others approach cyber-security from an economic perspective. *See* THE LAW AND ECONOMICS OF CYBERSECURITY (Mark F. Grady & Francesco Parisi eds., 2006); Coyne & Leeson, *supra* note 14, at 473–77; Powell, *supra* note 14, at 498–501; Rosenzweig, *supra* note 14, at 7–11.

[20] *Cf.* Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. 575 (2010) (proposing an administrative law framework for understanding domestic intelligence).

problems—the same sorts of challenges the modern administrative state encounters in a variety of other contexts.

For instance, cyber-security resembles environmental law in that both fields are primarily concerned with negative externalities. Just as firms tend to underinvest in pollution controls because some costs of their emissions are borne by those who are downwind, they also tend to underinvest in cyber-defenses because some costs of intrusions are externalized onto others. An attack on a power plant will not harm just the intended target; it will also harm the company's customers and those with whom the company has no relationship. Because firms do not bear the full costs of their vulnerabilities, they have weaker incentives to secure their systems. Cyber-security also resembles an antitrust problem. Antitrust law seeks to prevent anticompetitive behavior, and it traditionally has been skeptical of coordination among competitors. Some interfirm cooperation could improve cyber-security—sharing information about vulnerabilities and threats, for example, or developing industry-wide security standards. Yet firms are reluctant to do so because they fear antitrust liability. Cyber-security raises tort problems as well. Products liability law uses the threat of money damages to incentivize firms to take reasonable precautions when designing their products, but this threat is almost entirely absent in the cyber-security context. Companies face little risk of liability to those who are harmed by attacks on their systems or products, and they therefore have weaker incentives to identify and patch vulnerabilities. Finally, cyber-security resembles public health. A key goal of public health law is prevention—keeping those who have contracted a disease from spreading it to the healthy, a form of negative externality. Public health law uses vaccinations to promote immunity, biosurveillance to detect outbreaks, and quarantines to contain infectious diseases. Cyber-security has similar goals—ensuring that critical systems are immune to malware, quickly detecting outbreaks of malicious code, and preventing contaminated computers from infecting clean systems—and could use similar tools.

Approaching cyber-security from a regulatory vantage point does not just yield a richer analytical framework. It also expands the range of possible responses. If cyber-insecurity resembles problems that arise in other regulatory contexts, then perhaps some of their solutions can be adapted here; the more frameworks available, the longer the menu of policy choices. Taken together, these disciplines suggest four groups of responses: (1) monitoring and surveillance to detect malicious code, (2) hardening vulnerable targets and enabling them to defeat intrusions, (3) building resilient systems that can function during attacks and recover quickly, and (4) responding in the aftermath of attacks.

First, public health law's distributed biosurveillance network might be used as a model for detecting cyber-intrusions. Rather than empowering a single regulator to monitor Internet traffic for outbreaks of malicious code, private firms could be tasked with reporting information about the

vulnerabilities and threats they experience in the same way hospitals report to public health authorities. To incentivize participation in this distributed surveillance network, firms might be offered various subsidies (on the theory that cyber-security data is a public good that the market will tend to underproduce) and liability protections (such as an exemption from the antitrust laws). Second, we might harden targets by adopting industry-wide security standards for companies that operate critical infrastructure. These protocols should not be issued in the form of traditional regulatory commands. Instead, as is sometimes the case in environmental law and other fields, the private sector should actively participate in formulating the standards. Tort law has a role to play as well: threats of liability and offers of immunity might be used to incentivize firms to implement the protocols. Third, because it is inevitable that some cyber-attacks will succeed, it is important that critical systems are able to survive and recover. Public health law offers several strategies for improving resilience. Systems that are infected with malware might be temporarily isolated to prevent them from spreading the contagion. Or firms might build excess capacity into their systems that can be deployed in emergencies—the equivalent of stockpiling vaccines and medicines. Finally, although retaliation is thoroughly addressed in the existing criminal law and armed conflict literatures, there is one possible response that deserves brief mention here: "hackbacks," in which a victim counterattacks the attacker. Because the counterattack might fall on a third party whose system has been conscripted by the intruder, hackbacks can incentivize those third parties to prevent their systems from being so commandeered. Hackbacks also might weaken attackers' incentives: if assailants know that counterattacks can render their intrusions ineffective, they are less likely to commit them in the first place.

This Article proceeds in three parts. Part I considers whether private companies are investing socially optimal amounts in cyber-defenses. Part II describes four regulatory frameworks—environmental law, antitrust law, products liability law, and public health law—and explains their relevance to cyber-security. Part III surveys solutions used by these regulatory disciplines and considers how to adapt them for the cyber-security context.

Several preliminary observations are needed. First, I use the terms "cyber-attack" and "cyber-intrusion" interchangeably to denote any effort by an unauthorized user to affect the data on, or to take control of, a computer system. As used here, the terms include all of the following: "viruses" (a piece of code that "infects a software program and then ensures that the infected program reproduces the virus"[21]); "worms" ("a stand-alone program that replicates itself"[22]); "logic bombs" (malware that

[21] O'Neill, *supra* note 19, at 246; *accord* Katyal, *Criminal Law*, *supra* note 10, at 1023; Sklerov, *supra* note 19, at 14–15.

[22] Katyal, *Criminal Law*, *supra* note 10, at 1024; *accord* Sklerov, *supra* note 19, at 15. Viruses and worms are similar. A principal difference is that viruses require human action to propagate—such as

"tells a computer to execute a set of instructions at a certain time or under certain specified conditions"[23]); and distributed denial-of-service (DDOS) attacks (in which a "master" computer conscripts "zombies" and orders them to disable a victim by flooding it with traffic[24]). Second, this Article emphatically is not a paean to traditional command-and-control regulation. The conventional wisdom is to avoid cyber-security regulation,[25] in part because of doubts about the government's ability to manage such a dynamic field. But, as I hope to show in the following pages, cyber-security need not, and in many cases should not, be pursued with heavy-handed regulatory tools. It is possible to promote better cyber-defenses with private law, such as by modifying traditional tort law doctrines. As for public law, regulation need not take the form of rigid legal commands backed by the threat of sanction; regulatory objectives often can be attained by appealing to private firms' self-interest—by offering positive incentives to improve their defenses, not just by punishing them when they fall short. The private sector's poor defenses may represent a market failure, as some have argued,[26] but "[t]here's not much point in replacing a predictable market failure with an equally predictable government failure."[27]

I. AN EFFICIENT LEVEL OF CYBER-SECURITY

Our national security depends on the security of our critical infrastructure.[28] A cyber-attack on these assets, most of which are held by private firms, could be devastating: with a few keystrokes, adversaries could hack into banks and corrupt customer data, take control of power plants and bring down the electricity grid, open the floodgates of dams, and take telecommunications networks offline.[29] Or worse. Despite the magnitude of the threat, the conventional wisdom is that the private sector is not adequately protecting itself.[30] This section surveys the available

clicking on a link or opening an attachment—but worms replicate on their own. CLARKE & KNAKE, *supra* note 1, at 81; Katyal, *Criminal Law*, *supra* note 10, at 1024; O'Neill, *supra* note 19, at 247.

[23] Katyal, *Criminal Law*, *supra* note 10, at 1025; *accord* O'Neill, *supra* note 19, at 248.

[24] STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 202–03 (2010); BRENNER, *supra* note 1, at 38–39; CLARKE & KNAKE, *supra* note 1, at 13–14; Lin, *supra* note 19, at 70.

[25] *See* CLARKE & KNAKE, *supra* note 1, at 108–09; *see also* Derek E. Bambauer, *Ghost in the Network*, 164 U. PA. L. REV. (forthcoming 2014) (manuscript at 6), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2232471 ("[C]ybersecurity is underregulated.").

[26] *See* BAKER, *supra* note 24, at 237; CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 50; Katyal, *Digital Architecture*, *supra* note 15, at 2285.

[27] BAKER, *supra* note 24, at 237; *accord* Coyne & Leeson, *supra* note 14, at 490; Powell, *supra* note 14, at 507.

[28] *See* AM. BAR ASS'N, *supra* note 18, at 6–8; BRENNER, *supra* note 1, at 223.

[29] *See* BRENNER, *supra* note 1, at 137–54; CLARKE & KNAKE, *supra* note 1, at 64–68; Stewart Baker, *Denial of Service*, FOREIGN POL'Y (Sept. 30, 2011), http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service?print=yes&hidecomments=yes&page=full.

[30] *See infra* notes 34–41 and accompanying text.

evidence on the extent of private cyber-security expenditures. It then predicts that ordinary firms in competitive markets (like online retailers) are more likely to be investing socially optimal amounts in cyber-defense, while strategically significant firms in uncompetitive markets (like public utilities) are more likely to be underinvesting.

The optimal level of cyber-intrusions is not zero, and the optimal level of cyber-security expenditures is not infinity. From an economic perspective, the goal is to achieve an efficient level of attacks, not to prevent all attacks.[31] Suppose that the expected cost to society of a given cyber-attack—its cost discounted by the probability that it will occur—is $5 billion. It would be efficient for society to invest up to $5 billion in countermeasures to prevent the attack. If the necessary countermeasures cost more than $5 billion, the cost of preventing the attack would exceed the resulting security gains.[32] Relatedly, some intrusions are more problematic than others. Cyber-security is a form of risk management, where risk is a function of three variables: vulnerabilities, threats, and consequences.[33] A company with easily hacked systems, that faces a high probability of attacks from sophisticated foreign intelligence services, and whose compromise would cause severe social harm raises very different problems than a company with relatively robust defenses, that is unlikely to face skilled intruders, and whose compromise would have few consequences for society.

Are individual firms, and society as a whole, investing the right amount in cyber-defense? Most observers believe that firms are underinvesting—and are missing the mark by a wide margin. Richard Clarke proclaims the private sector response an "unmitigated failure,"[34] and scholars generally agree.[35] Very little empirical data is available, but the consensus view has at least some anecdotal support. Studies conducted in

---

[31] Coyne & Leeson, *supra* note 14, at 477–78.

[32] *Id.* at 478.

[33] *See, e.g.*, Rosenzweig, *supra* note 14, at 7.

[34] CLARKE & KNAKE, *supra* note 1, at 104.

[35] *See* AM. BAR ASS'N, *supra* note 18, at 9; Banks & Parker, *supra* note 7, at 9; Katyal, *Criminal Law*, *supra* note 10, at 1019; Bruce Schneier, Computer Security: It's the Economics, Stupid (May 16, 2002) (unpublished manuscript), *available at* http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/. *But see* Coldebella & White, *supra* note 14; Smith, *supra* note 17, at 173 n.12. Some scholars argue that companies are providing a suboptimally *high* level of cyber-security. Benjamin Powell reports that a 2000 study found that firms would invest in cyber-defenses if they were expected to produce a 20% return on investment, which was considerably lower than the 30% return on investment typically required for information technology investments. Powell, *supra* note 14, at 504. What mechanism could account for a tendency to overinvest? A firm's IT department has incentives to overstate the vulnerabilities the company faces, as cyber-security fears translate into a larger share of the company's budget; for outside security vendors, such fears mean brisker business. Bambauer, *Conundrum*, *supra* note 12, at 604–06; Calkins, *supra* note 19, at 198–99; Ross Anderson, Unsettling Parallels Between Security and the Environment (May 16, 2002) (unpublished manuscript), *available at* http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/.

2009 and 2011 by McAfee, a computer security firm, revealed low levels of investment in cyber-defense. The studies found that many firms regard cyber-security as little more than "a last box they have to check,"[36] and that they neglect network security because they find it too expensive.[37] In particular, McAfee found that companies often have weak authentication requirements[38]—tools that can verify that the person who is accessing a system is who he says he is, and is authorized to access the system. Even fewer have systems that can monitor network activity and identify anomalies.[39] Other studies reveal that some companies' defenses are so poor they don't even know when they've suffered an attack. Verizon reported that "fully 75 percent of the intrusions they investigated were discovered by people other than the victims and 66 percent of victims did not even know an intrusion occurred on the system."[40] Finally, a 2011 study by the Ponemon Institute found "that 73 percent of companies surveyed had been hacked, but 88 percent of them spent more money on coffee than on securing their Web applications."[41]

Are these levels of investment efficient? Whether a particular firm is making socially optimal investments in cyber-security—and the related issue of who should pay for that company's cyber-defenses—is a function of two intersecting questions. First, what is the defending firm? Is it a regular company in a competitive market, an operator of critical infrastructure in an uncompetitive market, or something in between? Second, who is the anticipated attacker? Is it a recreational hacker, a foreign intelligence service, or someone in between?

---

[36] MCAFEE & CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 15, at 1.

[37] MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 14 (2009), *available at* http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.

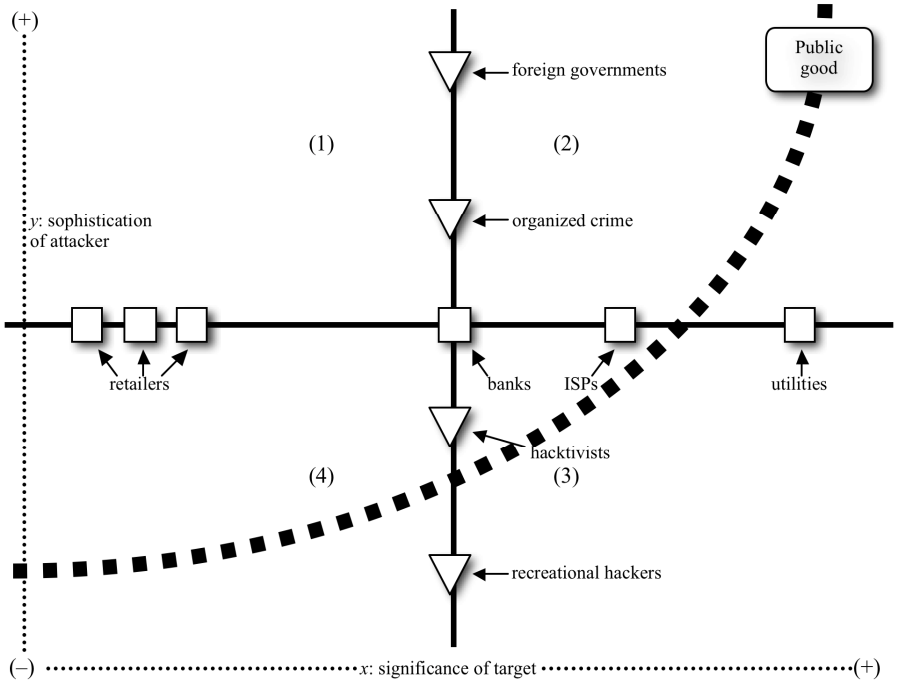
[38] *See* MCAFEE & CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 15, at 14.

[39] *Id.* at 15. It would be a mistake to read too much into these findings. The study's methodology was to survey business executives in about a dozen countries, MCAFEE, *supra* note 37, at 1, 41 n.1; MCAFEE & CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 15, at 3, and it "was not designed to be a statistically valid opinion poll with sampling and error margins." MCAFEE, *supra* note 37, at 1. Moreover, a computer security company obviously stands to benefit from public perceptions that security is lacking.

[40] Rattray et al., *supra* note 8, at 155; *accord* Jensen, *Cyber Warfare*, *supra* note 15, at 1536.

[41] BRENNER, *supra* note 1, at 239.

The range of possibilities can be depicted in a simple graph:



The *x*-axis depicts the firms that might be subject to a cyber-attack. They are arranged from left to right in order of increasing strategic significance. A strategically significant company is one whose compromise would result in substantial social harms. On the far left are relatively insignificant firms in competitive markets—markets in which many companies offer the same good or service, and where disappointed consumers therefore may defect from one to another. An example would be online retailers, such as Amazon.com. To the right are financial institutions, which rate high on the strategic significance scale. Former Director of National Intelligence Mike McConnell predicted that an attack on a single bank "would have an order-of-magnitude greater impact on the global economy" than 9/11.[42] Banks operate in fairly competitive markets, as consumers can easily move their accounts from one to another. Another step to the right are Internet Service Providers (ISPs) and telecommunications carriers. They, too, are strategically significant. When Russia crippled Georgia's communications systems during their 2008 war, citizens "could not connect to any outside news or information sources and

[42] David E. Sanger et al., *U.S. Plans Attack and Defense in Web Warfare*, N.Y. TIMES, Apr. 28, 2009, at A1 (quoting former Director of National Intelligence Mike McConnell); *accord* Sklerov, *supra* note 19, at 19–20.

could not send e-mail out of the country."[43] These markets are less competitive; consumers typically have only a handful of Internet providers or telephone companies to choose from. At the far right are power companies and other public utilities. These firms rate high on the strategic significance scale. A cyber-attack on the power grid would be truly catastrophic. The industrial control, or SCADA,[44] systems used by power plants and other utilities are increasingly connected to the Internet.[45] Hackers could exploit this connectivity to disrupt power generation and leave tens of millions of people in the dark for months.[46] They could even destroy key system components like turbines.[47] In 2009, the Stuxnet worm—"the most sophisticated cyberweapon ever deployed"[48]—caused similar physical damage to Iran's nuclear program.[49] Utility markets are uncompetitive. Municipalities typically have only one power company or natural gas supplier, and there is no meaningful prospect that disappointed consumers will switch to a competitor.

The *y*-axis depicts the assailants that might commit a cyber-attack. They are arranged from bottom to top in order of increasing sophistication. A sophisticated attacker is capable of compromising the most secure systems; unsophisticated attackers are only able to compromise relatively unsecured systems. At the bottom are recreational hackers—intruders out for "a digital joy ride."[50] One step above are "hacktivists." Hacktivists are relatively skilled hackers who use cyber-intrusions to advance a political

---

[43] CLARKE & KNAKE, *supra* note 1, at 19; *see also* BRENNER, *supra* note 1, at 39–40; Jensen, *Cyber Warfare*, *supra* note 15, at 1540.

[44] The acronym stands for "supervisory control and data acquisition." CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 54; CLARKE & KNAKE, *supra* note 1, at 98; Randal C. Picker, *Cybersecurity: Of Heterogeneity and Autarky*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY, *supra* note 19, at 115, 126.

[45] *See* BRENNER, *supra* note 1, at 97; CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 54; Steven R. Chabinsky, *Cybersecurity Strategy*, 4 J. NAT'L SEC. L. & POL'Y 27, 27 n.1 (2010); Condron, *supra* note 19, at 407; Coyne & Leeson, *supra* note 14, at 474; Sklerov, *supra* note 19, at 18.

[46] *See* BRENNER, *supra* note 1, at 105; CLARKE & KNAKE, *supra* note 1, at 99; Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391, 404–05 (2010); Ellen Nakashima & Steven Mufson, *Hackers Have Attacked Foreign Utilities, CIA Analyst Says*, WASH. POST, Jan. 19, 2008, at A4.

[47] *See* BRENNER, *supra* note 1, at 110; CLARKE & KNAKE, *supra* note 1, at 100; Gable, *supra* note 2, at 59–60; ECONOMIST, *supra* note 3, at 28.

[48] William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; *accord* BRENNER, *supra* note 1, at 102; Ellen Nakashima, *U.S. Systems Are Vulnerable to Hackers*, WASH. POST, Oct. 2, 2011, at A3; Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011, 7:00 AM), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[49] BRENNER, *supra* note 1, at 103; Bambauer, *Conundrum*, *supra* note 12, at 585–86; John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES, Sept. 27, 2010, at A6.

[50] Dunlap, *supra* note 12, at 358.

agenda; they typically do not group themselves into formal organizations.[51] An example is "Anonymous," a loose association that in late 2010 launched DDOS attacks on financial institutions that refused to let customers send money to WikiLeaks, an antisecrecy group that had published a number of classified documents.[52] Next are organized crime syndicates, such as those operating out of Russia.[53] They, too, are fairly sophisticated. They engage in cyber-intrusions primarily for financial gain and by definition they are structured organizations.[54] International terrorists might be placed here as well, though they have shown little enthusiasm or aptitude for cyber-attacks thus far.[55] However, al Qaeda reportedly established "an academy of cyber-terrorism" in Afghanistan,[56] and computers taken from members contained information about SCADA systems in the United States.[57] At the top are foreign governments' militaries and intelligence services. These are the most sophisticated adversaries of all, and they are capable of breaking into even highly secure systems. Internet giant Google recently saw its Gmail service penetrated by Chinese spies who wanted to eavesdrop on the Dalai Lama.[58] Similarly, RSA—a software firm that issues online security credentials for the Pentagon, defense contractors, and other sensitive enterprises—was compromised so badly (probably by China) that it had to offer new credentials to all its customers.[59]

The curve roughly predicts the combinations of victims and attackers that are likely to occur. Quadrant (4) involves high-frequency, low-severity attacks. Retailers and other relatively insignificant firms will be targeted fairly often by comparatively unsophisticated recreational hackers and, perhaps, by more sophisticated hacktivists who disapprove of their corporate policies. (The Anonymous attacks on banks are a good example.) Quadrant (2) involves attacks that are low-frequency and high-severity. More strategically significant firms like ISPs and public utilities will face attacks from sophisticated militaries and intelligence services, and perhaps

---

[51] *See* Byron Acohido, *Hacktivists Will Be Busy This Year, Experts Warn*, USA TODAY, Jan. 11, 2012, at 1B.

[52] Somini Sengupta, *16 People Arrested in Wave of Attacks on Web Sites*, N.Y. TIMES, July 20, 2011, at B2.

[53] Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, WASH. POST, Oct. 13, 2007, at A15.

[54] *See* BRENNER, *supra* note 1, at 7–8, 25.

[55] Condron, *supra* note 19, at 405; Dunlap, *supra* note 12, at 359–60.

[56] Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY, *supra* note 19, at 259, 259–60.

[57] BRENNER, *supra* note 1, at 106.

[58] *See* BAKER, *supra* note 24, at 208–13; BRENNER, *supra* note 1, at 46–47; Bambauer, *Ghost*, *supra* note 25, at 2–3; Ellen Nakashima, *Google to Enlist NSA to Ward Off Attacks*, WASH. POST, Feb. 4, 2010, at A1; Rosenzweig, *supra* note 14, at 6.

[59] Baker, *supra* note 29, at 2–3.

from organized crime syndicates seeking to extract blackmail payments. These attacks will occur rarely, but they are likely to be devastating. In quadrant (3), recreational hackers and hacktivists might launch attacks against utilities and similarly significant enterprises, but these targets are probably less attractive to them than they are to foreign militaries or intelligence services.[60] In quadrant (1), foreign governments are unlikely to target insignificant firms like retailers, because they gain little by compromising them, though organized crime may do so (again, for blackmail purposes).

We are now in a position to make predictions about various companies' cyber-security expenditures. The closer we are on the curve to the lower left corner, the higher the probability that the firm is investing a socially optimal amount in cyber-defense. This is so in part because the expected social cost of an attack on an ordinary company is fairly low. Society will not grind to a halt if Amazon.com is knocked offline; bookworms might experience minor annoyance but they will still be able to buy a copy of *Gilead* from Barnes & Noble. In addition, these companies are unlikely to face attacks by skilled and determined foreign governments, so it is not necessary for them to spend huge sums of money on the very best and most impregnable defenses. The efficient level of cyber-security investment for them thus is fairly low. Importantly, market forces may provide these firms with meaningful incentives to protect their systems against cyber-attacks. Retailers, banks, and similar companies operate in competitive markets. The risk of customer exit provides them with strong incentives to cater to customer demand. If consumers want the companies with which they do business to provide better security against cyber-attacks—the jury is out on that question, incidentally[61]—they will have good reason do so.[62]

---

[60] Zetter, *supra* note 48 ("[C]ontrol systems aren't a traditional hacker target, because there's no obvious financial gain in hacking them . . . .").

[61] *Compare* BRENNER, *supra* note 1, at 225–26 ("[S]oftware consumers buy on price, and they haven't been willing to pay for more secure software."), *and* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 946–47 (2007) (noting that consumers often lack direct relationships with the entities to which retailers outsource data processing and which are often the targets of intrusions), *with* Dunlap, *supra* note 12 (arguing that the growth in online retail will incentivize companies to invest in reliable computer security technology), *and* Doug Lichtman & Eric P. Posner, *Holding Internet Service Providers Accountable*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY, *supra* note 19, at 221, 256 ("[W]orms and viruses . . . impose[] a cost on the average user and thus reduce[] the incentive to subscribe.").

[62] Note that current liability rules both diminish and augment these incentives. The Federal Wiretap Act makes it a crime to intercept electronic communications, and some ISPs fear that this prohibition prevents them from filtering botnet traffic or other malware; the threat of liability undermines their incentives to improve the security of their systems. *See infra* notes 201–08 and accompanying text. By contrast, the Gramm–Leach–Bliley Act requires banks, on pain of significant money damages, to protect customer data against unauthorized access; the threat of liability amplifies their incentives to improve the security of their systems. *See infra* notes 209–17 and accompanying text.

The closer we are on the curve to the upper right corner—low-frequency, high-severity cyber-attacks—the lower the probability that the firm is adequately investing in cyber-security. First, the expected social cost of such an intrusion is monumental. The consequences of an attack on, say, the power grid would reverberate throughout the economy, causing harm to the utility, its customers, and countless third parties. Because the expected cost of an attack on these firms is so high, it is efficient to invest greater sums in securing them against intruders. In addition, the modest, low-cost defenses that are usually capable of thwarting recreational hackers will do nothing to prevent intrusions by foreign governments; more expensive countermeasures are needed to protect against these exceptionally sophisticated adversaries. The socially optimal level of cyber-security investment for these firms is thus fairly high.

Second, power companies and other utilities are not subject to market forces that might incentivize them to improve their cyber-defenses. Utilities face little if any competition; a given customer typically will be served by only one power company. Customer exit is essentially impossible, and the utility therefore has weaker incentives to supply what its customers demand. This absence of beneficial market forces may help explain why public utilities often fail to implement even relatively costless security measures.[63] Many electric companies use vendor default passwords to protect their SCADA systems,[64] and a recent study found that they take an average of 331 days to implement security patches for these systems.[65] Perhaps not coincidentally, hackers—most likely Chinese and Russian spies—have been able to insert logic bombs into the power grid.[66]

If this analysis is correct, then strategically significant firms in uncompetitive markets are less likely to adequately invest in cyber-security than ordinary firms in competitive markets. The question then becomes who should be responsible for securing these most sensitive companies against the most dangerous adversaries. Economists often argue that risk should be allocated to the low cost avoider.[67] If the government can reduce a vulnerability more efficiently than a firm, it should pay; if the firm can reduce the vulnerability more efficiently, it should pay. But there is no single low cost avoider in this context. Defending critical infrastructure

---

[63] Availability bias is another reason why firms might tend to underinvest in cyber-defense. *See generally* Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk Regulation*, 51 STAN. L. REV. 683 (1999) (describing availability bias). The United States has not experienced a major cyber-incident that has captured the public's imagination, so firms might irrationally discount the probability that they will suffer a catastrophic attack. *See* MCAFEE, *supra* note 37; John Grant, *Will There Be Cybersecurity Legislation?*, 4 J. NAT'L SEC. L. & POL'Y 103, 111 (2010).

[64] MCAFEE & CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 15, at 8.

[65] BRENNER, *supra* note 1, at 98.

[66] Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J., Apr. 8, 2009, at A1.

[67] *See* LAWRENCE LESSIG, CODE VERSION 2.0, at 169–70 (2006); Katyal, *Criminal Law*, *supra* note 10, at 1095–96.

against sophisticated cyber-attackers is a task that features dueling comparative advantages. Private firms typically know more than outsiders, including the government, about the architecture of their systems, so they often are in a better position to know about weaknesses that intruders might exploit.[68] The private sector thus has a comparative advantage at identifying cyber-vulnerabilities. On the other hand, the government's highly skilled intelligence agencies typically know more than the private sector about malware used by foreign governments and how to defeat it.[69] The government thus has a comparative advantage at detecting sophisticated attacks and developing countermeasures. This suggests that responsibility for defending the most sensitive systems against the most sophisticated adversaries should be shared.

What might such a partnership look like? All private firms might be asked to provide a baseline level of cyber-security—modestly effective (and modestly expensive) defenses that are capable of thwarting intrusions by adversaries of low to medium sophistication. The government would then assume responsibility for defending public utilities and other sensitive enterprises against catastrophic attacks by foreign militaries and other highly sophisticated adversaries.[70] This division of labor—basic security provided by firms, supplemental security provided by the government—is in a sense the opposite of what we see in realspace criminal law. In realspace, the government offers all citizens a baseline level of protection against criminals in the form of police officers, prosecutors, and courts. Individuals may supplement these protections at their own expense, such as by installing alarm systems in their homes or hiring private security guards.[71] This arrangement also is consistent with our intuitions about the respective roles of government and the private sector in times of conflict.[72] Consider another realspace analogy: in World War II, factories were not expected to install anti-aircraft batteries to defend themselves against Luftwaffe bombers.[73] Nor should we expect power plants to defend themselves against foreign governments' cyber-attacks. Protecting vital national assets from destruction by foreign militaries is a quintessential, perhaps *the* quintessential, government function.[74]

The division of labor I suggest also seems sound from an economic standpoint. If a firm invested in extraordinarily expensive cyber-defenses

---

[68] *See infra* notes 272–75 and accompanying text.

[69] *See infra* notes 276–78 and accompanying text.

[70] *See* Trachtman, *supra* note 56, at 272; Jeremy A. Rabkin & Ariel Rabkin, *To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict*, HOOVER INST. 4 (2012), http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf.

[71] *See* Rosenzweig, *supra* note 14, at 20.

[72] *See* CLARKE & KNAKE, *supra* note 1, at 144.

[73] Rosenzweig, *supra* note 14, at 25.

[74] BRENNER, *supra* note 1, at 223; CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 15; *see* Katyal, *Digital Architecture*, *supra* note 15, at 2282.

capable of thwarting doomsday attacks by foreign intelligence services, it would effectively be subsidizing the rest of the population. The company would capture some benefits of increased security, but a large portion of the benefits would be in the form of a positive externality conferred on others.[75] In other words, the firm would be providing a public good, a good that is both nonrivalrous and nonexcludable.[76] Economic theory predicts that public goods will be underprovided on the market;[77] a standard response is to subsidize their production.[78] Here, the government might provide a sensitive enterprise with a subsidy equal in value to its costs of defending against the most sophisticated cyber-attackers.[79] This subsidy could take many forms. The government could either pay for the firm's defenses directly or reimburse it for its cyber-security expenditures. Or the company could be offered various tax credits, deductions, and other benefits. Or it could be granted immunity from certain forms of legal liability. (In that case, the subsidy would not run from society as a whole, but from those who were injured by the firm's otherwise unlawful conduct and whose entitlement to redress had been extinguished. This sort of subsidy is potentially regressive.) Or the government might provide the company with intelligence about the types of attacks it may face. This sort of subsidy appears to be occurring already: the National Security Agency (NSA) reportedly is providing malware signature files to Google and certain banks to help them detect sophisticated intrusions into their systems.[80]

In short, private companies—especially firms that operate critical infrastructure in uncompetitive markets—may not be adequately investing in defenses against the most devastating forms of cyber-attacks. The next section explores several regulatory models that might be consulted when devising an appropriate response.

II. CYBER-SECURITY FRAMEWORKS, CONVENTIONAL AND UNCONVENTIONAL

Cyberspace is beset by externalities.[81] An externality is "an effect on the market the source of which is external to the market";[82] it occurs when

---

[75] Supriya Sarnikar & D. Bruce Johnsen, *Cyber Security in the National Market System*, 6 RUTGERS BUS. L.J. 1, 16–17 (2009).

[76] *See infra* notes 137–38 and accompanying text.

[77] *See infra* note 139 and accompanying text.

[78] *See, e.g.*, Nojeim, *supra* note 14, at 128.

[79] Amitai Aviram, *Network Responses to Network Threats*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY, *supra* note 19, at 143, 149, 156; Bambauer, *Conundrum*, *supra* note 12, at 658; Rosenzweig, *supra* note 14, at 25.

[80] *See infra* notes 277–78 and accompanying text.

[81] *See* Picker, *supra* note 44, at 115.

[82] Niva Elkin-Koren & Eli M. Salzberger, *Law and Economics in Cyberspace*, 19 INT'L REV. L. & ECON. 553, 563 (1999).

an actor's conduct results in the imposition of a cost or benefit on a nonconsenting third party. Externalities can be either positive or negative. "Positive externalities occur whenever an activity generates benefits that the actor is unable to internalize," such as through prices; "[n]egative externalities occur when one's activity imposes costs on others" that likewise are not transmitted through prices.[83] Economic theory predicts that the market will oversupply negative externalities relative to socially optimal levels "because the producer will internalize all benefits of the activity but not all of the costs."[84] It also predicts that the market will undersupply positive externalities because third parties will free ride.[85] Externalities thus represent a form of market failure.[86] The standard government response to a negative externality is to discourage the responsible conduct (e.g., with taxation or regulation); the standard response to a positive externality is to encourage the responsible conduct (e.g., with a subsidy).[87]

Cyber-security can be understood in these terms. If a company suffers an intrusion, much of the harm will fall on third parties; the attack results in a negative externality.[88] It can be extraordinarily difficult to internalize these costs. The class of persons affected by the intrusion will often be so large that it would be prohibitively expensive to use market exchanges to internalize the resulting externalities; the transaction costs are simply too great. Nor can tort law internalize the costs, as firms generally do not face liability for harms that result from cyber-attacks on their systems or products.[89] Because many companies do not bear these costs, they ignore them when deciding how much to spend on cyber-defense and therefore tend to underinvest relative to socially optimal levels. (This is true both of companies that produce computer products, such as software manufacturers, and companies that use them, such as ISPs and utility companies.) Cyber-security also involves positive externalities.[90] A company that secures itself against intruders makes it harder for assailants to commandeer its systems to attack others. Investments in cyber-defense thus effectively subsidize other firms. Because the investing company doesn't capture the full benefit of its expenditures, it has weaker incentives to secure its systems. And because other companies are able to free ride on the investing firm's expenditures, they have weaker incentives to adopt defenses of their own.

---

[83] *Id.*

[84] Coyne & Leeson, *supra* note 14, at 479.

[85] *Id.*

[86] *Id.*; *see also* Timothy F. Malloy, *Regulating by Incentives*, 80 TEX. L. REV. 531, 534 n.13 (2002).

[87] Coyne & Leeson, *supra* note 14, at 479; Rosenzweig, *supra* note 14, at 10.

[88] *See infra* notes 126–32 and accompanying text.

[89] *See infra* notes 190–94 and accompanying text.

[90] *See infra* notes 134–44 and accompanying text.

These externality and free-rider problems are largely overlooked in the law review literature. The vast majority of commentary regards cyber-security as a problem of the criminal law or the law of armed conflict.[91] The problem is not that these conventional approaches are mistaken. The problem is that they are incomplete. Treating cyber-security as a matter for cops or soldiers brings certain challenges into sharper focus. But it tends to obscure other problems—problems that may be illuminated if we consult alternative regulatory frameworks, such as environmental law, antitrust law, products liability law, and public health law. In short, a wider selection of analytical lenses allows us to fully comprehend cyber-security challenges in all their complexity. The following sections will explore these frameworks and their relevance for cyber-security.

A. The Conventional Approaches: Law Enforcement and Armed Conflict

Scholars typically use a pair of analytical frameworks to understand cyber-attacks: criminal law and the law of armed conflict. Consider the former first. Broadly speaking, the criminal law seeks to protect people from unjustified acts of violence against their persons or property. The criminal law pursues this objective by imposing sanctions, such as incarceration, on those adjudged to have violated the law. These penalties will punish those who have transgressed society's moral code (retribution), dissuade the perpetrator or others from committing similar offenses in the future (specific or general deterrence), isolate the dangerous perpetrator from society (incapacitation), or teach the misguided perpetrator the error of his ways (rehabilitation). Cyber-attacks fit into this conceptual framework fairly comfortably. A person who hacks into another's computer may have thereby violated any number of laws, such as the federal Computer Fraud and Abuse Act.[92] Society regards this sort of conduct as sufficiently blameworthy that it proscribes it and subjects those who engage in it to criminal penalties of varying severity.

Scholars who approach cyber-security from a law enforcement perspective focus on the "whodunit" questions. Who was responsible for launching this particular attack? Was it an individual hacker or a larger criminal enterprise? This framework also emphasizes jurisdictional questions.[93] Which courts properly may exercise subject matter jurisdiction over a given cyber-attack?[94] State courts, federal courts, or perhaps international tribunals? Should jurisdiction be determined by the location of the target? By the location of the attacker? By the location in which the effects of the attack are felt? Should cyber-attacks be subject to universal

---

[91] *See* sources cited *supra* note 19.

[92] 18 U.S.C.A. § 1030 (West Supp. 2012).

[93] *See* Gable, *supra* note 2, at 99–117.

[94] *See* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE 163–71 (2009); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1200–01 (1998).

jurisdiction—the notion that a court may try certain crimes regardless of where in the world they occurred?[95] How might courts gain personal jurisdiction over those suspected of committing the attack, especially if they are overseas? Do existing extradition treaties cover the range of offenses that cyber-criminals might commit? Should the United States negotiate new bilateral agreements with key international partners, such as our European allies, or with countries in which cyber-attacks are likely to originate, such as China and Russia? Or should there be a multilateral global convention on cyber-crime, one that will facilitate extradition of suspects from their home countries to the states in which they will stand trial for their alleged crimes?

The law enforcement framework also emphasizes punishment and deterrence.[96] Certain economic theories of criminal law posit that a person's willingness to commit crimes is a function of the expected penalty for that activity—i.e., the sanction for the particular offense discounted by the probability that the person will get caught.[97] The greater the sanction, and the greater the likelihood of detection and punishment, the less likely a person will choose to commit that crime. The question then becomes what should be done to increase the deterrent effect of laws that proscribe various cyber-intrusions. Should the penalties for violating these statutes be increased? Should society invest more resources in detecting cyber-crime, thereby increasing the probability that perpetrators will be caught and punished?[98] Or should lawmakers pursue "cost deterrence," the objective of which is to increase the costs one must incur to perpetrate cyber-crime?[99]

The second conventional approach regards cyber-attacks from the standpoint of the law of armed conflict (LOAC). The LOAC, also known as international humanitarian law (IHL), is a body of international law that regulates a state's ability to use force in several ways. First, it sets forth the circumstances in which a state lawfully may engage in armed conflict—the *jus ad bellum* regulations. For instance, the United Nations Charter forbids signatories "from the threat or use of force against the territorial integrity or political independence of any state,"[100] but also recognizes an inherent right

---

[95] *See generally* Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 HARV. INT'L L.J. 183, 190–92 (2004) (describing universal jurisdiction).

[96] *See* AM. BAR ASS'N, *supra* note 18, at 13; Gable, *supra* note 2, at 65; Katyal, *Criminal Law*, *supra* note 10, at 1006, 1011, 1040; O'Neill, *supra* note 19, at 265–68; K.A. Taipale, Cyber-Deterrence 18 (Jan. 1, 2009) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045.

[97] *See generally* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968) (analyzing the economically optimal level of enforcement).

[98] *See id.* at 169–95; George J. Stigler, *The Optimum Enforcement of Laws*, 78 J. POL. ECON. 526, 527 (1970).

[99] Katyal, *Criminal Law*, *supra* note 10, at 1006, 1012, 1039–40; *see also* O'Neill, *supra* note 19, at 265–88.

[100] U.N. Charter art. 2, para. 4.

to use force in self-defense against an "armed attack."[101] Second, the LOAC regulates what kinds of force may be used during an authorized armed conflict—the *jus in bello* regulations. For instance, a state may not deliberately kill civilians or destroy civilian infrastructure (the "distinction" or "discrimination" principle), may not inadvertently inflict harm on civilian populations and structures that is disproportionate to the importance of the military objective ("proportionality"), and may not cause more harm to legitimate targets than is needed to achieve the military objective ("necessity").[102]

Scholars who see cyber-security as an armed conflict problem typically focus on determining who was responsible for a particular attack.[103] Was this attack launched by a state or an international terrorist organization, in which case the LOAC may permit some form of military retaliation? Or was it carried out by criminals, in which case the distinction principle likely would rule out a military response? If the attacker was in fact a state or terrorist group, which one? Was it China, or maybe Russia, or perhaps North Korea? Or was it al Qaeda, or al Qaeda in the Arabian Peninsula, or Hezbollah? Until the identity of the assailant is known, it will be unclear against whom to retaliate—or whether retaliation is lawful at all.[104]

Another set of important questions concerns how to characterize a cyber-incident. Is a given intrusion espionage or an attack? It can be quite difficult to answer that question because the steps an intruder would take to steal information often are identical to the steps it would take to bring down a system. If the intrusion is properly understood as an attack, does it rise to the level of an "armed attack" that triggers the right of self-defense?[105] Should these questions be resolved with an "instrument-based" test, which counts a cyber-intrusion as an armed attack when it causes harms that previously could have been caused only by a kinetic attack?[106] Or a less demanding "effects-" or "consequence-based" test, which counts a cyber-intrusion as an armed attack when it has a sufficiently harmful effect on the targeted state?[107] Or an even less demanding "intent" test, which counts a

---

[101] U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs . . . .").

[102] *See generally* ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE 261–66 (2007) (describing LOAC principles); Eric A. Posner, *A Theory of the Laws of War*, 70 U. CHI. L. REV. 297, 298–99 (2003) (same).

[103] Graham, *supra* note 19, at 92; Lin, *supra* note 19, at 77.

[104] Condron, *supra* note 19, at 414.

[105] *Id.* at 412–13; Graham, *supra* note 19, at 90–92; Jensen, *Computer Attacks*, *supra* note 19, at 221; Lin, *supra* note 19, at 74. *See generally* Sklerov, *supra* note 19, at 50–59 (discussing various analytical models under which a cyber-attack could be considered an "armed attack").

[106] Graham, *supra* note 19, at 91; Sklerov, *supra* note 19, at 54.

[107] *See* Graham, *supra* note 19, at 91; Schmitt, *supra* note 19, at 913–15; Sklerov, *supra* note 19, at 54–55.

cyber-intrusion as an armed attack whenever it evinces a hostile intent, regardless of whether it causes actual damage?[108] The LOAC approach also addresses possible responses. When a nation suffers a cyber-attack, is it limited to responding with a cyber-intrusion of its own?[109] Or may a victim retaliate by launching a kinetic attack?[110] How severe must the cyber-attack be before a kinetic response would be justified?

Other problems for the LOAC arise from the fact that much of the world's critical infrastructure is dual use—it serves a state's civilian population but the state's political leadership and armed forces also rely upon it.[111] In the United States, for instance, civilian networks carry up to 98% of the federal government's communications traffic,[112] including 95% of defense-related traffic.[113] When, if ever, may a combatant direct a cyber-attack at an adversary's dual-use infrastructure?[114] Finally, the LOAC focuses on deterrence. Given the differences between cyber-conflicts and kinetic ones, how can a state dissuade its adversaries from committing cyber-attacks? Key differences include the difficulty in determining who was responsible for a given intrusion, the possibility that a retaliatory cyber-strike might end up harming innocent third parties more than the actual assailant, and the fact that different nations are more or less dependent on cyber-infrastructure and therefore have more or less to lose from an exchange of cyber-weapons.[115]

A central problem for both the law enforcement and armed conflict approaches to cyber-security is determining the identity of the assailant. Attribution is extraordinarily difficult; the challenges are "staggering"[116] and "[n]o one has come close to solving" them.[117] The problem is inherent

---

[108] WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129–31 (1999). Some scholars describe the intent test as a form of "strict liability." *See, e.g.*, Graham, *supra* note 19, at 91; Sklerov, *supra* note 19, at 55. This seems incorrect. A strict liability regime imposes liability solely on the basis of the social harm produced by the actor's conduct, without reference to his mens rea. WAYNE R. LAFAVE, CRIMINAL LAW § 5.5 (5th ed. 2010). It would be more accurate to say that the intent test imposes liability solely on the basis of mens rea, without any requirement that the actor's conduct result in social harm.

[109] *See* Condron, *supra* note 19, at 415–16; Graham, *supra* note 19, at 90.

[110] Jensen, *Computer Attacks*, *supra* note 19, at 229–30.

[111] CLARKE & KNAKE, *supra* note 1, at 242; Brown, *supra* note 13, at 193–94.

[112] Jensen, *Cyber Warfare*, *supra* note 15, at 1534.

[113] Condron, *supra* note 19, at 407; Jensen, *Computer Attacks*, *supra* note 19, at 211.

[114] *See* CLARKE & KNAKE, *supra* note 1, at 243; Brown, *supra* note 13, at 194; Jensen, *Cyber Warfare*, *supra* note 15, at 1543–46.

[115] CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 25–27; *see also* Lynn, *supra* note 19, at 99–100; James P. Terry, *Responding to Attacks on Critical Computer Infrastructure*, INT'L L. STUD. 421, 432–33 (2002).

[116] Jensen, *Computer Attacks*, *supra* note 19, at 234.

[117] Lin, *supra* note 19, at 77; *see also* Dycus, *supra* note 11, at 163; Katyal, *Criminal Law*, *supra* note 10, at 1047–48; O'Neill, *supra* note 19, at 275.

in the basic architecture of the Internet. The Internet's TCP/IP protocol[118] was designed to move packets of data as efficiently as possible; it is utterly unconcerned with who sent them.[119] As such, it is fairly easy for attackers to obscure their true identities by routing their intrusions through a series of dispersed intermediary computers.[120] These attribution difficulties can severely frustrate the law enforcement and armed conflict approaches to cyber-security.

B. Cyber-security as an Environmental Law Problem

Given the limits of the conventional cyber-security frameworks, it's advisable to look for guidance in other legal disciplines—particularly the regulatory disciplines that confront the same sorts of problems seen in the cyber-security context. For instance, a principal goal of environmental law is to regulate externalities. Various forms of environmental degradation involve negative externalities—i.e., spillover costs that are imposed on third parties and that are not transmitted through prices.[121] Sometimes these externalities are geographic: toxins emitted by a factory in Ohio might affect residents of New York.[122] Sometimes they are temporal: carbon emissions today might affect the planet's climate for future generations.[123] The critical point is that these costs are borne by people other than those who are responsible for the pollution, and market transactions cannot readily be used to internalize the costs onto the polluter. Many scholars therefore believe that regulatory controls are necessary.[124] These controls often take the form of strict limits on regulated activity backed by the threat of civil damages or criminal sanctions,[125] though less coercive forms of regulation exist.

Cyber-security can be understood in terms of negative externalities.[126] A given firm—whether it is a company that produces or uses computer

---

[118] TCP/IP is the primary way data is transmitted online. It stands for "Transmission Control Protocol/Internet Protocol."

[119] LESSIG, *supra* note 67, at 44; Bambauer, *Conundrum*, *supra* note 12, at 595–96.

[120] BRENNER, *supra* note 1, at 32; Gable, *supra* note 2, at 101; Graham, *supra* note 19, at 92; Ruth G. Wedgwood, *Proportionality, Cyberwar, and the Law of War*, 76 INT'L L. STUD. 219, 227 (2002).

[121] *See supra* notes 81–87 and accompanying text.

[122] *See, e.g.*, Massachusetts v. EPA, 549 U.S. 497, 521–25 (2007).

[123] Richard J. Lazarus, *A Different Kind of "Republican Moment" in Environmental Law*, 87 MINN. L. REV. 999, 1000, 1005 (2003).

[124] *See, e.g.*, *id.* at 1005–06 (citing a "need for government regulation because of the spatial and temporal spillovers caused by unrestricted resource exploitation").

[125] *See, e.g.*, Clean Water Act, 33 U.S.C. § 1319(b)–(c) (2006) (providing civil and criminal penalties); Clean Air Act, 42 U.S.C. § 7413(b) (2006) (providing civil penalties).

[126] Anderson, *supra* note 35. One potential difference between pollution and cyber-security is that pollution is a harmful byproduct of socially beneficial activity (such as manufacturing) whereas cyber-attacks involve intentionally malicious conduct. *See* Rattray et al., *supra* note 8, at 171. Yet cyber-intrusions likewise may be seen as a harmful byproduct of beneficial activity. A cyber-attack on a computer is a byproduct of the computer being connected to the Internet. And connecting a computer to

products—will not bear the full costs of its cyber-insecurities. (By "cyber-insecurity," I mean a firm's failure to implement defenses capable of defeating a cyber-attack.) Instead, some of these costs are borne by third parties; they are partially externalized.[127] Imagine a cyber-attack that disables a power plant. The intrusion would harm the utility as well as consumers who buy electricity from it[128]—hospitals, manufacturers, and others. The attack also would harm a number of third parties who have no relationship with the power company—hospital patients, downstream manufacturers in the supply chain, and so on. These "indirect effects of a cyber attack are almost always more important to the attacker than the direct effects."[129] And it would be prohibitively expensive to internalize them through market exchanges; the transaction costs would be staggering, in part because it is extraordinarily difficult to identify the universe of third parties affected by the intrusion.

The fact that many costs of cyber-attacks are externalized is enormously significant. Some commentators have argued that firms have strong "financial incentives to protect [their systems] from cyber attacks."[130] Those incentives are weaker than might be supposed. A firm that is deciding how much to invest in securing its systems will not account for the costs that an attack will impose on third parties.[131] Firms tend to oversupply pollution, since they capture all the benefits of the associated productive activity but not all of the resulting costs. In a similar way, firms tend to oversupply cyber-insecurity—or, to say the same thing, they tend to undersupply cyber-defense—because they internalize all of the benefits but only some of the costs.[132] Firms thus may invest less in cyber-defense than would be optimal from a societal standpoint.

The point can be illustrated with a simple hypothetical. Imagine a cyber-attack that will result in $1 million in expected costs for the target firm and $10 million in expected costs for third parties. From a societal standpoint, it would be worthwhile to invest up to $11 million to prevent the attack. But from the company's standpoint, it would only be worthwhile to invest up to $1 million. If the firm spent more than that, the cost of the

---

the Internet is socially beneficial because it produces network effects; by joining the network, the user increases its value to all users. POST, *supra* note 94, at 47–49.

[127] AM. BAR ASS'N, *supra* note 18; Schwartz & Janger, *supra* note 61, at 928; Anderson, *supra* note 35; Jim Harper, *Government-Run Cyber Security? No Thanks*, CATO INST. (Mar. 13, 2009), http://www.cato.org/publications/techknowledge/governmentrun-cyber-security-no-thanks; Rosenzweig, *supra* note 14, at 9–10.

[128] Aviram, *supra* note 79, at 155; Lin, *supra* note 19, at 68.

[129] Lin, *supra* note 19, at 68.

[130] Nojeim, *supra* note 14, at 134; *accord* Coldebella & White, *supra* note 14, at 236, 241; Dunlap, *supra* note 12; Yang & Hoffstadt, *supra* note 15, at 203.

[131] *See* AM. BAR ASS'N, *supra* note 18; Coyne & Leeson, *supra* note 14, at 479; Rosenzweig, *supra* note 14, at 9–10.

[132] Coyne & Leeson, *supra* note 14, at 480.

precautions would exceed the benefit to the firm and the firm would be conferring uncompensated benefits on third parties. Thus, there is a gap between the welfare of the company and the welfare of society as a whole. Levels of cyber-security investment that are efficient for particular firms may turn out to be inefficient for society at large.[133]

Cyber-security can also be understood as a positive externality. When a firm expends resources to defend itself against intruders, that investment can make other users' systems marginally more secure as well. This is so because the defenses not only help prevent harm to the company's system, they also help prevent the firm's system from being used to inflict harm on others' systems.[134] If Pepsi's network is well-defended, it is less likely to be infected by a worm and thus less likely to transmit the malware through the Internet to Coke. The effect is to decrease the overall incidence of infection, but the investing firm does not capture the full benefit. A classic positive externality. Cyber-defenses can differ from realspace defenses in this respect. If I install an alarm in my home, that might prevent burglars from breaking into my house, but it will not necessarily decrease the overall incidence of burglary. The alarm might simply displace the burglar who would have targeted me onto my neighbor[135]—a form of negative externality. By contrast, cyber-defenses can make my system more secure at the same time they increase the overall security of the Internet.[136]

Relatedly, some aspects of cyber-security resemble public goods.[137] A public good is both nonrivalrous (one person's use of the good does not reduce its availability for use by others) and nonexcludable (the owner of the good cannot prevent particular persons from using it).[138] A classic example of a public good is a large municipal park: the park is open to all comers, and one person enjoying a crisp fall afternoon on a bench generally does not prevent anyone else from doing the same. Some scholars argue that cyber-security information—information about the vulnerability of a particular system, or the most effective way to counter a particular cyber-

---

[133] Sarnikar & Johnsen, *supra* note 75, at 15.

[134] Katyal, *Criminal Law*, *supra* note 10, at 1081–82; O'Neill, *supra* note 19, at 278; Rosenzweig, *supra* note 14, at 9.

[135] O'Neill, *supra* note 19, at 278; *see also* Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 46 (2005); Katyal, *Criminal Law*, *supra* note 10, at 1081.

[136] *But see* Bruce K. Kobayashi, *Private Versus Social Incentives in Cybersecurity: Law and Economics*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY, *supra* note 19, at 13, 16; Rosenzweig, *supra* note 14, at 9.

[137] *See* CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 50; Mulligan & Schneider, *supra* note 19, at 71; Powell, *supra* note 14, at 498–99.

[138] Elkin-Koren & Salzberger, *supra* note 82, at 559; James Grimmelmann, *The Internet Is a Semicommons*, 78 FORDHAM L. REV. 2799, 2806 (2010); Rosenzweig, *supra* note 14, at 8–9; *see also* Harold Demsetz, *The Private Production of Public Goods*, 13 J.L. & ECON. 293, 295 (1970) (distinguishing between nonrivalrous goods, which are properly characterized as public goods, and nonexclusive goods, which are properly characterized as "collective goods").

threat—is a public good that the market will tend to underproduce.[139] There is also a sense in which defensive measures themselves are public goods. Like a municipal park, cyber-defenses can be nonrivalrous.[140] When Pepsi expends resources to secure its computer network, that does not decrease the amount of security available for Coke. Doing so can actually *increase* security for third parties, as attackers will be unable to use Pepsi's secured system as a platform to launch attacks on other companies. Cyber-defenses also can be nonexcludable.[141] When Pepsi secures its system against conscription into a botnet—a network of "zombie" computers ordered by the "master" to commence a DDOS attack[142]—it isn't possible to specify which third parties will enjoy the benefit of Pepsi's immunity; for instance, protecting Coke but not Snapple. *All* such users are thereby protected from attacks launched from Pepsi's system.

Environmental law and the underlying economic principles it reflects thus provide an important framework to understand the tendency of some firms to neglect cyber-defense. It's a free-rider problem.[143] Companies tend to underinvest in cyber-defenses for the same reason they tend to underinvest in pollution controls—because insecurities that result in successful attacks produce negative externalities that are borne by third parties. Firms also tend to underinvest in cyber-defenses because such expenditures create positive externalities and provide opportunities for free riding. "The individual undertaking the security precautions does not internalize all the benefits, and will seek to free-ride off of the efforts taken by others"; as a result, "theory predicts that security will be undersupplied on the market."[144] Understood in these terms, the challenge for a cyber-security regime is to internalize the externalities—to ensure that firms that fail to secure their systems are made to bear the resulting costs.

C. . . . as an Antitrust Problem

Antitrust law is another useful framework for understanding cyber-security problems. The ultimate goal of antitrust, promoting consumer welfare, is achieved by restraining businesses from engaging in anticompetitive conduct. Antitrust law is especially concerned about the possibility that firms will take coordinated action that undermines

---

[139] Kobayashi, *supra* note 136, at 16; Rosenzweig, *supra* note 14, at 9. *But see* Amitai Aviram & Avishalom Tor, *Overcoming Impediments to Information Sharing*, 55 ALA. L. REV. 231, 234–35, 240–47 (2004) (arguing that information can be a rivalrous good, insofar as sharing it can cause a firm to "los[e] a competitive edge over rivals that benefit from the information").

[140] Kobayashi, *supra* note 136, at 20–21; Trachtman, *supra* note 56, at 270.

[141] Trachtman, *supra* note 56, at 270.

[142] *See supra* note 24.

[143] Aviram & Tor, *supra* note 139, at 238; Elkin-Koren & Salzberger, *supra* note 82, at 559; Trachtman, *supra* note 56, at 281; *see also* CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 50. *But see* Powell, *supra* note 14, at 504–05.

[144] Coyne & Leeson, *supra* note 14, at 480.

competition—an agreement to divide a market, for instance. Antitrust also is apprehensive about information sharing among competitors; such exchanges, it is feared, "can facilitate anti-competitive collusion or unilateral oligopolistic behavior."[145] Hence Section 1 of the Sherman Act sweepingly prohibits "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States."[146]

Antitrust law often subjects coordinated conduct by multiple competitor firms to stricter scrutiny than isolated conduct by a single firm.[147] The law condemns many such arrangements—namely, "naked" restraints or coordinated actions that are "formed with the objectively intended purpose or likely effect of increasing price or decreasing output in the short run"[148]—under a per se rule against cartelization.[149] With a per se rule, there is no need to inquire whether a particular arrangement actually has anticompetitive effects. Antitrust law takes a shortcut and simply presumes that the conduct is harmful.[150] This approach may lead to the occasional false positive—coordinated action that is actually beneficial to consumers but that nevertheless is condemned as unlawful. But the conventional wisdom is that the costs of these false positives would be dwarfed by the decision costs of distinguishing the small number of naked restraints that are procompetitive from the much larger number that are anticompetitive.

Yet some interfirm cooperation is beneficial to consumers,[151] and antitrust law can struggle to determine whether a given instance of joint action is pro- or anticompetitive.[152] In the cyber-security context, various forms of coordination and information sharing can help firms better defend themselves against intrusions, and thus prevent consumers from incurring losses. Firms in a particular industry might agree to exchange threat information.[153] An ISP that discovers it has been victimized by a particular form of malware could alert others to be on the lookout for the same threat. Or firms could share vulnerability information.[154] A power plant that learns that its SCADA system can be compromised by a particular type of intrusion could tell other companies about the vulnerability. Firms also

---

[145] Aviram & Tor, *supra* note 139, at 236.

[146] 15 U.S.C. § 1 (2006).

[147] HERBERT HOVENKAMP, FEDERAL ANTITRUST POLICY: THE LAW OF COMPETITION AND ITS PRACTICE § 5.1, at 211 (4th ed. 2011); *see also id.* § 5.1b, at 214–16.

[148] *Id.* § 5.1a, at 212.

[149] *Id.* § 5.1, at 211.

[150] *Id.* § 5.1, at 211–12.

[151] *See id.* § 5.1, at 211; Aviram & Tor, *supra* note 139, at 231.

[152] *See* HOVENKAMP, *supra* note 147; Aviram & Tor, *supra* note 139, at 236.

[153] *See* Emily Frye, *The Tragedy of the Cybercommons*, 58 BUS. LAW. 349, 368–69 (2002); Lichtman & Posner, *supra* note 61, at 236.

[154] Aviram & Tor, *supra* note 139, at 263.

might share countermeasure information. A company might discover an especially effective way to defend against a DDOS attack, and the company might notify other firms to use the same technique. Finally, an industry might agree to establish a uniform set of cyber-security standards, along with monitoring and enforcement mechanisms to ensure that all members are implementing the agreed-upon measures. They might, in other words, form something like a cartel.

Which brings us to the problem. Coordinating on cyber-defense could give rise to antitrust liability, and firms therefore are reluctant to share information or to adopt common security standards.[155] These liability fears appear to be fairly widespread. A 2002 analysis found that, among the private sector's "major concerns about fully communicating cybervulnerabilities," one of the most important is "the potential for antitrust action against cooperating companies."[156] In a 2009 report, the American Bar Association (ABA) likewise recounted the concerns of several firms that "antitrust laws created a barrier to some forms of sharing" cyber-security information.[157] Government officials have reported the same fears. The White House's 2009 Cyberspace Policy Review acknowledged that some interfirm coordination takes place, but went on to report that "some in industry are concerned that the information sharing and collective planning that occurs among members of the same sector under existing partnership models might be viewed as 'collusive' or contrary to laws forbidding restraints on trade."[158]

These concerns seem well-founded. There are a number of scenarios in which cyber-security coordination could trigger liability under federal antitrust statutes. For instance, suppose that firms in a particular industry

---

[155] *Cf.* Jonathan H. Adler, *Conservation Through Collusion: Antitrust as an Obstacle to Marine Resource Conservation*, 61 WASH. & LEE L. REV. 3 (2004) (arguing that antitrust regulation discourages cooperative interfirm efforts to control effects of pollution on marine life).

[156] Frye, *supra* note 153, at 374. The other two reported concerns are "an increased risk of liability" and the "loss of proprietary information." *Id.*

[157] AM. BAR ASS'N, *supra* note 18, at 10.

[158] EXEC. OFFICE OF THE PRESIDENT, *supra* note 6, at 18–19. *But see* BRENNER, *supra* note 1, at 228 (dismissing the fear that cyber-security coordination might give rise to antitrust liability as "overblown"); Rosenzweig, *supra* note 14, at 16 (same). Cyber-security experts sometimes exchange information about threats and vulnerabilities notwithstanding the antitrust laws. For instance, an informal collaboration between researchers at Symantec, the computer security company, and several freelance computer experts in Europe revealed that Stuxnet, originally thought to be a "routine and unambitious" piece of malware, was in fact a sophisticated cyber-weapon aimed at Iran's nuclear program. Zetter, *supra* note 48. This episode is important for two reasons. First, it confirms that information sharing can produce significant cyber-security gains. Second, it suggests that information sharing is more likely to take place where there is little risk of antitrust liability. Symantec and European researchers could freely exchange information because they did not offer competing goods or services, so the arrangement was unlikely to be condemned as a contract, combination, or conspiracy in restraint of trade.

agree to implement a uniform set of cyber-security practices.[159] It is improbable that these new standards would be costless. Whether the companies have agreed to purchase and install new firewall software, or to transition from vulnerable commercial-off-the-shelf (COTS) systems to more expensive proprietary systems, the measures are likely to affect their bottom lines. Industry members might decide to absorb these increased costs, depending on the elasticity of consumer demand for the goods or services they offer. But they might further decide to pass on these costs to consumers, either in the form of a general price hike or as a free standing surcharge. Would the arrangement be lawful? This sort of venture may amount to price fixing in violation of Section 1 of the Sherman Act.[160] Even if the participating firms do not set a specific price for their products (e.g., everyone will now charge $50 for widgets instead of $45), they still establish a premium that will be assessed for their products (e.g., everyone will increase the price they charge for their widgets by $5). The economic effect is the same. Indeed, the arrangement may even amount to a "naked" restraint that results in reflexive condemnation under the per se rule.[161]

As a second example, consider an arrangement that imposes no new costs on consumers—at least not directly. Suppose firms in a particular industry agree to install intrusion-detection or -prevention capabilities to scan for malware on their networks.[162] These systems rely on a technique known as "deep-packet inspection," in which all data traversing the network is scanned and checked against signature files of known malware.[163] The effect is often to slow down the network's performance, sometimes dramatically.[164] Suppose further that the firms decide to absorb the costs of the monitoring or detection system rather than pass them on to their consumers. Would that forbearance save the arrangement from

---

[159] *Cf.* Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679 (1978) (invalidating an industry group's safety standards that prohibited members from engaging in competitive bidding).

[160] *See* 15 U.S.C. § 1 (2006).

[161] *See* HOVENKAMP, *supra* note 147, § 5.1a, at 212. The venture also might stand condemned as an unlawful tying arrangement. Tying occurs when a firm requires a consumer to purchase one product as a condition of purchasing another. *Id.* § 10.1, at 435. For instance, Canon refuses to sell you a camera unless you also buy a flash. Like naked restraints, tying arrangements are often reviewed under a per se rule, especially where the firm has market power. *But see* Jefferson Parish Hosp. Dist. No. 2 v. Hyde, 466 U.S. 2, 40 & n.10 (1984) (O'Connor, J., concurring in the judgment) (arguing that tying arrangements should be reviewed under a rule of reason). Transferring the increased costs of cyber-security to consumers might be seen as an effort to force them to buy a new security product in addition to the firm's basic product. Imagine a bank that previously would have offered financial services, such as the ability to use a credit card, for $45 a year. After the agreement, it now sells financial services *plus* enhanced security for $50 a year. Firms might fear that regulators and private litigants will regard that additional $5 as the price for a separate product, cyber-security, which consumers may or may not independently wish to purchase. *See* sources cited *supra* note 61.

[162] *See* POST, *supra* note 94, at 85.

[163] *See* CLARKE & KNAKE, *supra* note 1, at 161–62; LESSIG, *supra* note 67, at 55–56; Lynn, *supra* note 19, at 103.

[164] *See* CLARKE & KNAKE, *supra* note 1, at 81; Smith, *supra* note 17, at 180.

antitrust liability? Not necessarily. The shared security standards still plausibly could be described as an unlawful price-fixing agreement. While the participating companies have not agreed to raise prices directly, they have indirectly accomplished something similar; instead of requiring consumers to pay a *higher* price for the *same* product, the firms have agreed to require consumers to pay the *same* price for a *lesser* product (where speed is an important component of the product's value).

Notice that clear and unambiguous prohibitions on interfirm coordination may not be necessary to deter businesses from participating in joint cyber-security ventures. Mere uncertainty about the applicability of the antitrust laws—and the corresponding risk of liability—may be enough. The deterrent effect is likely to be especially strong because of the severe sanctions that may be imposed on antitrust defendants. Firms that are alleged to have violated federal antitrust laws face criminal prosecutions as well as federal civil actions,[165] state civil actions,[166] and lawsuits by aggrieved private parties.[167] Each type of civil litigation carries the prospect of treble damages payouts to the successful plaintiffs.[168] Private firms therefore will have good reasons to avoid coordinating their efforts to improve cyber-security.

To be sure, fear of antitrust liability is not the only reason firms are reluctant to coordinate and share information. The difficulties of forming and maintaining cartels are well-known. Among other problems, individual cartel members have strong incentives to cheat, such as by offering a greater quantity of product or by charging a different price than allotted by the cartel.[169] In the cyber-security context, businesses will have comparable incentives to shirk their responsibilities to implement any agreed-upon (and likely costly) security standards. In addition, firms may be especially reluctant to share information with their competitors.[170] If a firm discovers an effective way to defend its systems against a particular form of cyber-intrusion, that information gives it a comparative advantage over rivals that may not be as adept at protecting their own networks. Sharing the information with competitors enables them to free ride and thereby eliminates the firm's comparative advantage. As such, even if fears of antitrust liability were eliminated completely, it is doubtful that firms would fully cooperate with one another. Nevertheless, liability concerns appear to be a significant impediment to cyber-security coordination and

---

[165] § 15a.

[166] *Id.* § 15c.

[167] *Id.* § 15.

[168] *Compare id.* § 15(a) (treble damages in private lawsuits), *with id.* § 15a (treble damages in lawsuits by United States), *with id.* § 15c(a)(2) (treble damages in lawsuits by state attorneys general).

[169] *See* HOVENKAMP, *supra* note 147, § 4.1a, at 161–68.

[170] Aviram & Tor, *supra* note 139, at 252–54; *accord* Nathan Alexander Sales, *Share and Share Alike*, 78 GEO. WASH. L. REV. 279, 319–20 (2010).

information sharing. Reducing these fears would not by itself ensure cooperation, but might make it more likely at the margin.

D. . . . as a Products Liability Problem

Private investment in cyber-security also resembles a tort problem—more precisely, a products liability problem. Broadly speaking, the law of products liability has two complementary goals.[171] First, from an ex post perspective, the law seeks to compensate consumers injured by products that did not perform as expected. Second, from an ex ante perspective, products liability law uses the risk of money damages to incentivize firms to take reasonable precautions when designing and manufacturing products.

The branch of products liability law that is most relevant to cyber-security is design defects. In a design defect case, the theory is that "the intended design of the product line itself is inadequate and needlessly dangerous."[172] (By contrast, a manufacturing defect occurs when a product suffers from "a random failing or imperfection,"[173] such as a crack in a Coke bottle that causes it to explode,[174] and a marketing defect occurs when an otherwise safe product "become[s] unreasonably dangerous and defective if no information explains [its] use or warns of [its] dangers.")[175] In its infancy, products liability law typically assigned blame on a theory of strict liability.[176] A plaintiff could recover damages by establishing that a given product had a defective design and that he was injured by that defect; it wasn't necessary to show that the manufacturer was negligent, or otherwise blameworthy, in producing the defect.[177] The modern approach abandons strict liability in favor of a negligence standard.[178] How do courts determine whether a manufacturer was at fault when it produced a product with a design defect? One common approach is the risk–utility test.[179] The test, which has its roots in Learned Hand's negligence formula,[180] compares

---

[171] *See, e.g.*, DAN B. DOBBS, THE LAW OF TORTS § 353, at 975–76 (2000); WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 4–5 (1987).

[172] DOBBS, *supra* note 171, § 355, at 980; *accord* MICHAEL I. KRAUSS, PRINCIPLES OF PRODUCTS LIABILITY 81 (2011).

[173] DOBBS, *supra* note 171, § 355, at 979.

[174] *See* Lee v. Crookston Coca-Cola Bottling Co., 188 N.W.2d 426 (Minn. 1971).

[175] DOBBS, *supra* note 171, § 355, at 981.

[176] *See, e.g.*, Greenman v. Yuba Power Prods., Inc., 377 P.2d 897, 901 (Cal. 1963); RESTATEMENT (SECOND) OF TORTS § 402A (1965).

[177] DOBBS, *supra* note 171, § 353, at 974–75.

[178] *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 1 cmt. a, at 7 (1998); *see also* DOBBS, *supra* note 171, § 353, at 977; KRAUSS, *supra* note 172, at 40; LANDES & POSNER, *supra* note 171, at 292.

[179] RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 cmts. a & f, at 15–17; *see also* DOBBS, *supra* note 171, § 357, at 985–87 (describing the risk–utility test); LANDES & POSNER, *supra* note 171, at 291–92 (describing the test in terms of "cost–benefit").

[180] *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

"the risks of the product as designed against the costs of making the product safer."[181] If the risks can be reduced by a significant amount at a relatively low cost, a manufacturer that declines to do so is negligent. If the risks can be reduced only by a small amount at a relatively high cost, a manufacturer that declines to do so is not negligent.

Tort liability creates important incentives for manufacturers to prevent or eliminate design defects.[182] Imagine a company that makes residential furnaces; it is trying to decide whether to remedy a design defect that increases the probability that the furnaces will explode. The company will do so if the expected benefits of reducing the risk of explosion exceed the expected costs of making the fix. Without tort liability, the benefit of making defect-free furnaces is lower than it otherwise would be. Furnaces that occasionally explode would damage the firm's reputation, and some consumers likely would buy competitors' products instead. The manufacturer benefits to the extent it reduces these harms. But it does not face the prospect of paying money damages to homeowners whose houses burned down. The cost–benefit calculus looks very different once a products liability regime is in place. Tort liability increases a firm's expected benefit of remedying design defects—namely, the benefit of foregone money damages, discounted by the probability that they would be awarded. It thus increases the number of circumstances in which firms will find it welfare maximizing to improve the safety of their products. The result is that, at the margin, products will be safer than they otherwise would be.

Internet-related goods and services sometimes suffer from design defects that increase their vulnerability to cyber-attacks.[183] Perhaps the best known example is Microsoft Windows. The operating system software, which accounts for more than 90% of the PC market,[184] is notoriously riddled with vulnerabilities. These flaws stem in part from the software's size. In 2006, Microsoft projected that Windows Vista would feature some 50 million lines of code, compared to 35 million for Windows XP (released in 2001) and just 15 million for Windows 95 (released in 1995).[185] It is more or less inevitable that the programmers who write these millions of lines will make mistakes, and it can be quite difficult to detect and repair them.[186] (Given that it probably would cost a great deal to eliminate all of these vulnerabilities, the failure to do so may not be negligent under the

---

[181] DOBBS, *supra* note 171, § 357, at 985.

[182] *See* LANDES & POSNER, *supra* note 171, at 10–11 (discussing the deterrent effects of tort law).

[183] *See* Lichtman & Posner, *supra* note 61, at 255.

[184] Steve Lohr & John Markoff, *Windows Is So Slow, but Why?*, N.Y. TIMES, Mar. 27, 2006, at C1.

[185] *Id.*

[186] *See* DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 12 (1999); Bambauer, *Ghost*, *supra* note 25, at 9–10; Katyal, *Digital Architecture*, *supra* note 15, at 2264–65; Mulligan & Schneider, *supra* note 19, at 72.

risk–utility test.)[187] Other examples abound. Indeed, many of the vulnerabilities described in Part I can be understood as the results of design defects. Consider the decision by power companies to connect generators and other elements of the electrical grid to the Internet. This might be described as a form of defective system design, in that Internet connectivity exposes the nation's power grid to potentially catastrophic cyber-attacks in exchange for relatively modest benefits.[188] The same can be said of companies that continue to protect their SCADA systems with vendor-supplied default passwords[189]—a defect, incidentally, that could be remedied at a negligible cost.

The incentives to cure these design defects are fairly weak because poor cyber-security generally does not trigger civil liability.[190] One reason for this is a venerable chestnut of tort law known as the economic loss doctrine. The economic loss doctrine provides that, while a defendant who causes physical injuries is also liable for any resulting economic harms, he generally is not liable for freestanding economic harms.[191] Many of the harms that would result from a cyber-attack on, say, the power grid or the financial sector would be purely economic in nature. An automobile manufacturer might be unable to run its assembly line because the power is out, or a consumer might default on a loan because he can't make a payment online. Few of these harms would derive from a physical injury, and they therefore would not be actionable. For instance, in 2009, the Supreme Judicial Court of Massachusetts dismissed a lawsuit brought by credit unions against a retailer after hackers accessed the retailer's computer systems and stole customer credit card data.[192] The court agreed with the lower court's conclusion that, because "the plaintiffs suffered only economic harm due to the theft of the credit card account information," the "economic loss doctrine barred recovery on their negligence claims."[193]

---

[187] *But see* Lichtman & Posner, *supra* note 61, at 255 (arguing that improving the security of Windows "is simply a matter of investing more resources in product design as well as testing").

[188] *See supra* notes 44–49 and accompanying text.

[189] *See supra* notes 63–65 and accompanying text.

[190] *See* BRENNER, *supra* note 1, at 224; Schneier, *supra* note 35, at 2.

[191] *See* DOBBS, *supra* note 171, § 452, at 1282, 1285–87 (discussing the economic loss doctrine as well as exceptions and modifications to the rule); LANDES & POSNER, *supra* note 171, at 251. The rule has two familiar rationales: first, "financial harm tends to generate other financial harm endlessly and often in many directions" and liability "would be onerous for defendants and burdensome for courts," and second, the notion that "contract law is adequate to deal with the problem and also usually more appropriate." DOBBS, *supra* note 171, § 452, at 1283.

[192] *See* Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E.2d 36, 39, 49–51 (Mass. 2009).

[193] *Id.* at 46–47; *accord* Pa. State Emps. Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 330 (M.D. Pa. 2005) ("A plaintiff must show physical damage to property, not its tangible nature, to avoid the application of the economic loss doctrine."), *aff'd in part sub nom.* Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 176–78 (3d Cir. 2008). *But see* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys. Inc., 729 F.3d 421 (5th Cir. 2013) (concluding that New Jersey tort law did not

Cyber-attacks that cause physical injuries would remain actionable, as would any resulting economic harms. So, for instance, if an attacker exploited a design defect in a dam's control system and opened the floodgates,[194] the dam operator might be held liable for the deaths of the downstream landowners and any corresponding economic losses.

The problem also can be understood in Coasean terms.[195] Consider the famous example of a train that emits sparks that burn the wheat in neighboring fields.[196] Regardless of whether the legal entitlement is initially assigned to the railroad (a right to emit sparks) or the farmers (a right to be free from incinerated crops), the parties will bargain to reallocate the entitlement to its socially most efficient use, assuming that the transaction costs are sufficiently small. In the cyber-security context, the absence of tort liability essentially grants firms a legal right to refrain from taking precautions that would protect third parties from attacks on their systems or products. This may be an efficient allocation of the legal entitlement in some contexts, but not always. In these latter circumstances, companies and third parties theoretically should negotiate and establish a new legal right to be free from harm due to cyber-intrusions. But Coasean bargaining over cyber-security seems unlikely to occur because of the staggering transaction costs. It would be prohibitively expensive, if not impossible, for companies to bargain with everyone who conceivably could be injured by cyber-attacks on their systems or products.

Beyond tort, it is doubtful that other sources of law will threaten cyber-security shirkers with liability. Contract law does not seem well suited to the task. Software manufacturers typically do not offer warranties that their products are secure.[197] Indeed, some do not "sell" software at all. They merely grant a license, and users cannot install the software unless they click a button to accept terms and conditions that usually include a limit on the manufacturer's liability.[198] Likewise, federal law extends broad immunity to ISPs. Section 230 of the Communications Decency Act provides that an ISP will not "be treated as the publisher or speaker of any information provided by another information content provider."[199] At least one federal appellate court has interpreted this statute to foreclose a lawsuit alleging that an ISP negligently failed to prevent malware from being sent

bar recovery for economic harms resulting from a cyber-intrusion); Patco Constr. Co. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012) (upholding liability under contract governed by Uniform Commercial Code for economic harms resulting from a cyber-intrusion).

194 Frye, *supra* note 153, at 350; Sklerov, *supra* note 19, at 20.

195 *See* R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

196 *See id.* at 29–34.

197 *See* Frye, *supra* note 153, at 367.

198 *See* BRENNER, *supra* note 1, at 224.

199 47 U.S.C. § 230(c)(1) (2006).

over its network.[200] From the standpoint of a profit-maximizing firm, the expected benefits of remedying a cyber-vulnerability often will be lower than the expected costs. Without the prospect of tort liability, firms have weaker incentives to invest in measures to secure their systems and products against cyber-attacks.

Not only do liability fears fail to incentivize firms to take better precautions against cyber-attacks, they can actually discourage them from doing so. Companies sometimes are reluctant to better secure their systems because of concerns that these steps could expose them to civil liability. For instance, ISPs typically do not offer assistance if they discover that their customers' PCs have been infected by malware. ISPs often are able to tell, through routine traffic analysis, that a particular machine on the network is part of a botnet or has been infected by a worm.[201] "[B]ut they don't dare inform the customer (much less cut off access) out of fear that customers would . . . try to sue them for violating their privacy."[202] Doing so might even be a crime. The Federal Wiretap Act makes it unlawful to "intentionally intercept[] . . . any wire, oral, or electronic communication,"[203] and some companies fear that filtering botnet traffic or other malware might fall within this prohibition.[204] And while federal law makes an exception for ISPs that intercept communications to protect their own property,[205] there is no parallel exception for intercepts intended to protect the property of subscribers. Likewise, some ISPs use deep packet inspection to examine the data streams on their networks for malicious code. This is probably lawful under the exception mentioned above, or a separate exception for "mechanical or service quality control checks."[206] But even when they uncover malware, ISPs "have been reluctant to 'black hole' (or kill) malicious traffic because of the risk that they might be sued by customers whose service is interrupted."[207] Again, as in the antitrust context, even if the applicable service contracts or state and federal laws do not clearly forbid these measures, the mere risk of liability may be enough to dissuade firms from undertaking them.[208]

While firms with poor cyber-defenses generally do not face the prospect of civil lawsuits, there is one context in which a credible liability threat exists. The Gramm–Leach–Bliley Act of 1999 (GLB Act) imposes

---

[200] Green v. Am. Online (AOL), 318 F.3d 465, 470–72 (3d Cir. 2003). *See generally* Lichtman & Posner, *supra* note 61, at 251–52 (discussing *Green* case).

[201] *See* BRENNER, *supra* note 1, at 229; CLARKE & KNAKE, *supra* note 1, at 164–65.

[202] CLARKE & KNAKE, *supra* note 1, at 164–65; *accord* BRENNER, *supra* note 1, at 229; Coldebella & White, *supra* note 14, at 236–37.

[203] 18 U.S.C. § 2511(1)(a) (2006).

[204] BRENNER, *supra* note 1, at 229–30.

[205] § 2511(2)(a)(i).

[206] *Id.*

[207] CLARKE & KNAKE, *supra* note 1, at 163; *see also* MCAFEE, *supra* note 37, at 5.

[208] *See supra* notes 165–68 and accompanying text.

liability for data breaches in the financial services sector. The Act directs a group of federal agencies, such as the Federal Trade Commission (FTC) and the Federal Deposit Insurance Corporation, to issue data security regulations for financial institutions.[209] In particular, the Act mandates the adoption of "administrative, technical, and physical safeguards" that will, among other things, "insure the security and confidentiality of customer records and information" and "protect against unauthorized access to or use of such records."[210] The sanctions for violating these data security requirements can be severe. Gramm–Leach–Bliley does not enumerate specific penalties, but rather directs the enforcing agencies to apply the Act's requirements according to their respective enabling statutes.[211] Thus, for example, a bank subject to FTC jurisdiction would face a civil penalty of up to $16,000 for each violation.[212] If the FTC treated every customer affected by a cyber-intrusion as a separate violation, the penalties could very quickly become staggering.

Perhaps not coincidentally, financial institutions are widely believed to do a better job of protecting customer data than members of other industries.[213] Unlike other firms, which typically spend only modest sums on cyber-security, most banks devote "between 6 and 7 percent of their entire information technology budgets."[214] Financial institutions also are more likely to adopt specific security measures like intrusion-detection and -prevention systems, antivirus software, smart cards, and biometrics.[215] The unique risk of liability that banks face may be responsible, at least in part, for that record. The GLB Act has the effect of increasing the expected benefit of cyber-security—namely, avoiding potentially crippling civil penalties—and thus creates strong incentives for banks to invest in defenses. (Another explanation is the risk of customer exit. Unlike, say, the customers of public utilities, it is relatively easy for a depositor who fears cyber-intrusions to switch banks, so the bank has an incentive to maintain data integrity.)[216]

Of course, the GLB Act's emphasis on protecting consumer data might distort firms' cyber-security investments. Rather than expending resources on defenses against the attacks they regard as the most dangerous, or the

---

[209] *See* 15 U.S.C. §§ 6801(b), 6805 (2006). *See generally, e.g.*, FTC Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 (2012).

[210] § 6801(b); *see* Kenneth A. Bamberger, *Regulation as Delegation*, 56 DUKE L.J. 377, 391 (2006); Schwartz & Janger, *supra* note 61, at 920.

[211] *See* § 6805(b).

[212] 16 C.F.R. § 1.98.

[213] Frye, *supra* note 153, at 367–68; *see also* AM. BAR ASS'N, *supra* note 18, at 21; Powell, *supra* note 14, at 501–05. *But see* Gable, *supra* note 2, at 84 (emphasizing that the international financial system remains vulnerable to cyber-attack).

[214] Powell, *supra* note 14, at 502.

[215] *See id.* at 503.

[216] *See supra* notes 42–49 and accompanying text.

most likely to occur, financial institutions will tend to prioritize defenses against the one form of intrusion singled out by their regulators—the compromise of customer data.[217] The effect may be to ensure that firms are well-defended against one threat at the expense of increased exposure to many other threats.[218] Even so, Gramm–Leach–Bliley remains an example of how the risk of civil liability might be used to incentivize firms to improve at least some of their cyber-defenses.

E. . . . as a Public Health Problem

As several scholars have noted, in more or less detail, cyber-security can be thought of in terms of public health.[219] A critically important goal for any cyber-security regime is to keep attacks from happening and to contain their ill effects.[220] The same is true of public health, the ultimate goal of which is prevention.[221] Unlike medical practice, which typically has an ex post orientation toward treating illnesses that have already occurred, public health is primarily oriented toward ex ante solutions—preventing people from contracting infectious diseases, preventing pathogens from spreading, and so on. Broadly summarized, public health law, including the subset known as public health emergency law, involves government efforts "to persuade, create incentives, or even compel individuals and businesses to conform to health and safety standards for the collective good."[222] Some scholars defend these interventions on controversial paternalistic grounds. The notion is that the state may curtail individuals' freedoms to promote their own physical health and safety.[223] The more common justification is the risk of harm to others: the state may coerce persons who have contracted an infectious disease or are at risk of doing so to prevent them from transmitting the disease to, and thereby harming, others.[224] Seen in this light, a principal objective of public health law is to internalize negative

---

[217] Similar distortions may arise at the state level, as a number of states have enacted laws requiring designated companies to disclose breaches of customer data. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 283–87 (2005); *see also* Schwartz & Janger, *supra* note 61, at 917.

[218] *Cf.* BAKER, *supra* note 24, at 238–39 (noting that state law causes companies to divert resources to measures that would prevent having to disclose a breach, such as encrypting files, rather than focusing on keeping hackers out of the system); MCAFEE, *supra* note 37, at 29 (noting that disclosure laws "might be driving companies to make investment and policy decisions that will reduce the number of reportable incidents, rather than strengthening the overall security of the enterprise").

[219] IBM, *supra* note 19; Mulligan & Schneider, *supra* note 19; Rattray et al., *supra* note 8, at 151–68; *see also* Coyne & Leeson, *supra* note 14, at 480; Hunker, *supra* note 19, at 202–03; Katyal, *Criminal Law*, *supra* note 10, at 1081; Rosenzweig, *supra* note 14, at 19 & 32 n.83.

[220] *See* Katyal, *Community*, *supra* note 135, at 34; Katyal, *Criminal Law*, *supra* note 10, at 1078–79.

[221] LAWRENCE O. GOSTIN, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT 19 (2d ed. 2008).

[222] *Id.* at xxii.

[223] *Id.* at 50–54.

[224] *Id.* at 49.

externalities—in particular, the costs associated with spreading infections to others.

Public health law contemplates three specific measures that are relevant here: mandatory inoculations to reduce susceptibility to infectious diseases, biosurveillance to monitor for epidemics and other outbreaks, and isolation and quarantine to treat those who have been infected and prevent them from spreading the pathogen.[225] We will consider each in turn along with their potential relevance to cyber-security.

Inoculation, in which a healthy subject is exposed to a pathogen, helps prevent disease both directly (a person who is inoculated against a disease is thereby rendered immune) and indirectly (the person's immunity reduces the risk that he will transmit the disease to others). Inoculation mandates can take several forms. In the nineteenth and early twentieth centuries, state and local governments sometimes opted for direct regulation—a firm legal requirement that citizens must receive a particular vaccine, backed by the threat of sanctions.[226] In the 1905 case of *Jacobson v. Massachusetts*,[227] the Supreme Court upheld such a requirement against a lawsuit invoking the Fourteenth Amendment's privileges or immunities, due process, and equal protection clauses. According to the Court, mandatory inoculation is a permissible exercise of the states' police powers.[228] The modern approach usually involves a lighter touch. Now, state and local governments typically create incentives for citizens to undergo inoculation by making it a condition of eligibility for certain valuable benefits. The best known example is to deny children access to public schools unless they have been vaccinated.[229] The Supreme Court upheld such a scheme in 1922 in *Zucht v. King*.[230]

It isn't necessary to inoculate all members of a population to frustrate the transmission of a given disease. This is so because of "herd immunity." When large numbers of a population are immune to a given contagious disease, their immunity helps prevent the disease from spreading, even to those who are not immune.[231] The critical number is typically around 85% of the population, but it can be as low as 75% for some diseases, such as mumps, and as high as 95% for others, such as pertussis.[232] Herd immunity is a form of positive externality—those who undergo vaccination provide

[225] *Id.* at 11, 39.

[226] *See id.* at 379 (describing laws that required certain vaccinations as a precondition to attending public school).

[227] 197 U.S. 11 (1905).

[228] *Id.* at 24–30, 38.

[229] *See* GOSTIN, *supra* note 221, at 379–80, 382; Hunker, *supra* note 19, at 203.

[230] 260 U.S. 174, 176–77 (1922).

[231] Katyal, *Criminal Law*, *supra* note 10, at 1081; Mulligan & Schneider, *supra* note 19, at 76.

[232] *History and Epidemiology of Global Smallpox Eradication*, CTRS. FOR DISEASE CONTROL & PREVENTION 17, http://www.bt.cdc.gov/agent/smallpox/training/overview/pdf/eradicationhistory.pdf (last visited Sept. 5, 2013).

an uncompensated benefit to those who do not—which creates a potential free-rider problem.[233] Many people would prefer to enjoy the benefits of herd immunity without themselves undergoing vaccination, which is costly in terms of money, discomfort, and risk of reaction. This free-rider problem weakens each person's incentive to undergo vaccination, and overall vaccinations may drop below the levels needed to support herd immunity. State and local governments therefore sometimes use their coercive powers to require inoculation. (Another approach would be to provide subsidies to those who have been inoculated. Public school vaccination requirements can be understood in these terms; the government is subsidizing the education of children who are inoculated.)

Ensuring widespread immunity—not to disease, but to malicious code—is also an important goal of cyber-security. The average Internet-connected computer may be even more susceptible to infection by malware than the average person is to infection by a pathogen, because malicious code can propagate more efficiently than disease. Many pathogens are transmitted by person-to-person contact; you are unlikely to contract polio unless you come into close proximity with someone who is already infected. But one can contract malware from virtually any networked computer in the world. The Internet effectively brings dispersed systems into direct contact with one another. Alternatively, the Internet is a disease vector that, like mosquitoes and malaria, can transmit a contagion between dispersed systems. It is therefore essential for the elements at the edge of the network, such as the SCADA system that runs the local power plant, to maintain effective defenses against cyber-intrusions, such as isolating the power plant's controls from the public Internet. And there's the rub. As with herd immunity, cyber-security raises free-rider problems.[234] A user who takes steps to prevent his computer from being infected by a worm or impressed into a botnet thereby makes other systems more secure; if the user's machine is not infected, it cannot transmit the malware to others. But the user receives no compensation from those who receive this benefit; he does not internalize the positive externality. He therefore has weaker incentives to secure his system, as he—like everyone else—would prefer to free ride on others' investments. A critical challenge for any cyber-security regime is to reverse these incentives.

The second key element of public health law is biosurveillance. "Biosurveillance is the systematic monitoring of a wide range of health data of potential value in detecting emerging health threats . . . ."[235] Public health officials collect and analyze data to determine a given disease's

---

[233] *See* GOSTIN, *supra* note 221, at 378–79; Coyne & Leeson, *supra* note 14, at 480. *See generally supra* notes 143–44 and accompanying text (discussing the free-rider problem in the context of cyber-defense investments).

[234] *See supra* notes 143–44 and accompanying text.

[235] GOSTIN, *supra* note 221, at 291.

incidence, or "the 'rate at which new cases occur in a population during a specified period,'" as well as its prevalence, or "the 'proportion of a population that are cases at a point in time.'"[236] Effective biosurveillance is a vital first step in managing an epidemic or other outbreak.[237] Biosurveillance takes place through a partnership among the U.S. Centers for Disease Control and Prevention, the CDC's state level counterparts, and front line health care providers, such as hospitals, clinics, and individual medical practitioners. Many, if not all, states have enacted legislation requiring specified health care professionals to notify state authorities if their patients have contracted any number of infectious diseases,[238] such as smallpox or polio.[239] These reports typically include the patient's name, the type of disease, medical history, and other personal information.[240] State authorities then share the data with the CDC. These reports are not required by law, but most states appear to be fairly conscientious about them.[241] Public health law thus uses a system of distributed surveillance. No central regulator is responsible for collecting all the data needed to detect and respond to infectious disease outbreaks. Instead, the system relies on individual nodes within a far-flung network—from state agencies to hospitals to individual doctors—to gather the necessary information and route it to the CDC's central storehouse. The CDC then analyzes the data and issues alerts advising state agencies and medical practitioners about disease trends and offering recommendations about how to respond.[242]

The third public health intervention involves containing infectious diseases once an outbreak has occurred, and preventing them from spreading further.[243] Two key measures are isolation and quarantine.[244] The goal of each is to segregate from the population those who have contracted

---

[236] Rattray et al., *supra* note 8, at 152 (quoting Dan Geer, Measuring Security, Address at the 16th USENIX Security Symposium 132, 134 (Aug. 6, 2007), *available at* http://geer.tinho.net/usenix/).

[237] *See* IBM, *supra* note 19, at 11–12.

[238] *See* GOSTIN, *supra* note 221, at 295–96.

[239] *Summary of Notifiable Diseases—United States, 2009*, 58 MORBIDITY & MORTALITY WKLY. REP. 1, 3 (2011), *available at* http://www.cdc.gov/mmwr/pdf/wk/mm5853.pdf.

[240] GOSTIN, *supra* note 221, at 297.

[241] *Id.* at 296; Hunker, *supra* note 19, at 202–03.

[242] This reporting scheme is permissible under the Health Insurance Portability and Accountability Act privacy rule, which generally limits the use and disclosure of protected health information, *see* 45 C.F.R. § 164.502(a) (2012), but which contains an exception for disclosures to public health authorities, *see id.* § 164.512(b). The reporting is probably constitutional as well. The Supreme Court in *Whalen v. Roe*, 429 U.S. 589 (1977), upheld, against a Fourteenth Amendment challenge, a similar New York law requiring physicians to report information about drug prescriptions. *Id.* at 603–04, 606.

[243] *See* Rattray et al., *supra* note 8, at 154–55.

[244] Isolation and quarantine differ in subtle ways, though in colloquial usage the terms are essentially synonymous. Isolation involves separating persons who are known to be infected with a disease, for as long as the disease remains communicable. GOSTIN, *supra* note 221, at 429. Quarantine involves separating persons who, though asymptomatic, may have been exposed to a disease, for the period of communicability. *Id.*

or been exposed to an infectious disease, and thus prevent them from transmitting it to those who are well.[245] Isolation and quarantine are often coupled with mandatory treatment, which helps reduce the risk of further contagion; a person who has been cured of an infectious disease cannot transmit it to others.[246] The rationale for these interventions is the familiar harm principle—the risk that a person who has contracted or been exposed to a pathogen will infect others.[247] Isolation and quarantine thus seek to reduce negative externalities.

At the federal level, isolation and quarantine are accomplished under the Public Health Service Act of 1944. The Secretary of Health and Human Services has authority under the Act "to make and enforce such regulations as in his judgment are necessary to prevent the introduction, transmission, or spread of communicable diseases" into or within the United States.[248] The law further provides for "the apprehension, detention, or conditional release" of persons who may have been exposed to any one of several communicable diseases that the President has specified by executive order.[249] The list, which was updated most recently in 2005,[250] includes cholera, tuberculosis, plague, smallpox, SARS, and several other diseases.[251] Large-scale isolation and quarantine are rarely used; the most recent example is from the 1918 Spanish flu pandemic, which was carried out under different legal authorities.[252] However, isolation and quarantine are sometimes used for particular individuals. In May 2007, HHS issued an isolation order for an American with multidrug-resistant tuberculosis who flew from the Czech Republic to Canada and then crossed the land border into the United States.[253] Violations of the quarantine regulations carry criminal penalties, including a fine of up to $1000 and incarceration for up to a year.[254]

Both biosurveillance and isolation/quarantine carry important lessons for cyber-security. Like the public health system, effective cyber-defenses

---

[245] *Id.*

[246] *See id.* at 411–12.

[247] *Id.* at 414–15.

[248] 42 U.S.C. § 264(a) (2006).

[249] *Id.* § 264(b).

[250] Exec. Order No. 13,375, 70 Fed. Reg. 17,299 (Apr. 1, 2005).

[251] Exec. Order No. 13,295, 68 Fed. Reg. 17,255 (Apr. 4, 2003).

[252] *See Legal Authorities for Isolation and Quarantine*, CTRS. FOR DISEASE CONTROL & PREVENTION, http://www.cdc.gov/quarantine/aboutlawsregulationsquarantineisolation.html (last updated Jan. 10, 2012).

[253] *Cracks in the System—An Examination of One Tuberculosis Patient's International Public Health Threat: Hearing Before the Subcomm. on Labor, Health, & Human Servs., Educ. & Related Agencies of the S. Comm. on Appropriations*, 110th Cong. 14 (2007) (statement of Julie Gerberding, Director, Centers for Disease Control and Prevention), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110shrg41837/pdf/CHRG-110shrg41837.pdf.

[254] § 271(a).

depend on information about the incidence and prevalence of various kinds of malware. Users need to know what new forms of malicious code are circulating on the Internet in order to secure their systems against them. And measures resembling isolation and quarantine can help ensure that systems infected with malicious code do not spread the contagion to other, healthy computers.

There is, of course, a significant difference between infectious diseases and malicious computer code: diseases typically develop and spread on their own, whereas malware is created by human beings and sometimes requires human intervention to propagate. This is true as far as it goes, but the differences between cyberspace and realspace pathogens can be overstated. Infectious diseases can be engineered (e.g., biological weapons), and sometimes malware is able to spread on its own (e.g., a worm that is programmed to search for other computers on which to replicate itself[255]). Another potential obstacle is the tension between antique public health legislation and contemporary constitutional law. These statutes often restrict civil liberties and privacy to a degree rarely seen today,[256] and the judicial precedents upholding them against various constitutional challenges typically antedate the Supreme Court's modern civil rights and liberties jurisprudence. It is not clear that today's Court would uphold, say, mandatory vaccination of adults as readily as it did in 1905.[257] Yet even if public health law fits uneasily with modern constitutional law, it can still be a useful framework for cyber-security because, as explained below, the cyber versions of public health interventions can be friendlier to civil liberties and privacy than their realspace counterparts.[258]

III. REGULATORY PROBLEMS, REGULATORY SOLUTIONS

This concluding Part examines the responses of environmental, antitrust, products liability, and public health law to various challenges, and it considers how those solutions might be adapted for cyber-security. The possible responses to cyber-insecurity are determined by our antecedent choice of how to describe that problem. If we regard cyber-security from the standpoint of law enforcement and armed conflict, we will tend to favor the responses of law enforcement and armed conflict—stronger penalties for cyber-intrusions, retaliating with kinetic attacks, and so on. Those are plausible frameworks and equally plausible solutions. But they are not the only ones. A wider angle lens is needed.

---

[255] *See supra* note 22 and accompanying text.

[256] *See* GOSTIN, *supra* note 221, at 24.

[257] Jacobson v. Massachusetts, 197 U.S. 11, 39 (1905). *But see* GOSTIN, *supra* note 221, at 130 (proposing that the Court "indisputably" would reach the same result if it decided *Jacobson* today).

[258] *See infra* notes 285−86 and accompanying text.

Taken together, the regulatory frameworks described in Part II suggest that an effective cyber-security regime should include four components: (1) monitoring and surveillance to detect malicious code, (2) hardening vulnerable targets and enabling them to defeat intrusions, (3) building resilient systems that can function during an attack and recover quickly, and (4) responding in the aftermath of an attack.[259] There are two complementary objectives here: preventing intrusions from happening at all, and enabling firms to withstand the intrusions that do take place.[260] Stronger defenses would provide an obvious, first-order level of protection: better defense means less damage. They also would provide an important second-order level of protection: stronger defenses can help achieve deterrence. By enabling victims to defeat, survive, and recover from cyber-attacks, these measures increase the expected costs of an intrusion to an attacker and also decrease its expected benefits.[261] And that means weaker incentives to attack in the first place; why try to take down the power grid if the effort is likely to fail?

Of course, it is inevitable that some attacks will succeed. Some intrusions can be prevented or mitigated but others cannot, and any defensive scheme is necessarily imperfect.[262] This is so because offense is much less costly than defense in cyberspace. "Defending a modern information system" is like "defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere."[263] The goal therefore is not to develop impregnable defenses. Doing so may be impossible from a technological standpoint and, even if such defenses were feasible, they may be inefficiently costly.[264] Instead, the goal is to attain efficient levels of investment in defenses that are better at protecting society's critical systems than current defenses are.[265] Another important point is that cyber-defense is not a one-size-fits-all proposition. Security

---

[259] *Cf.* Trachtman, *supra* note 56, at 265 (describing the various goals of an effective cyber-security regime).

[260] BRENNER, *supra* note 1, at 214; CLARKE & KNAKE, *supra* note 1, at 159; Bambauer, *Conundrum*, *supra* note 12, at 673; Yochai Benkler, *Peer Production of Survivable Critical Infrastructures*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY, *supra* note 19, at 73, 76–77.

[261] CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 26; Bambauer, *Ghost*, *supra* note 25, at 7; Lynn, *supra* note 19, at 99–100; Taipale, *supra* note 96, at 36.

[262] CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 51; IBM, *supra* note 19, at 12; Bambauer, *Conundrum*, *supra* note 12, at 673; Bambauer, *Ghost*, *supra* note 25, at 5; Gable, *supra* note 2, at 65; Lynn, *supra* note 19, at 99; Sklerov, *supra* note 19, at 8; Taipale, *supra* note 96, at 9.

[263] Ross Anderson, *Why Information Security Is Hard—An Economic Perspective*, *in* 17TH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE: PROCEEDINGS 358 (2001), *available at* http://www.acsac.org/2001/papers/110.pdf; *accord* BAKER, *supra* note 24, at 213; Bambauer, *Ghost*, *supra* note 25, at 11; Jensen, *Cyber Warfare*, *supra* note 15, at 1536. *But see* Libicki, *supra* note 12, at 38.

[264] *See supra* notes 31−32 and accompanying text.

[265] DENNING, *supra* note 186.

measures should be tailored to the unique risks faced by specific firms or industries—their combinations of vulnerabilities, threats, and consequences.[266] The strongest, and presumably most costly, defenses should be reserved for the firms that are most vulnerable to cyber-attacks, that face the most severe threats (e.g., from foreign intelligence services as opposed to recreational hackers), and whose compromise would have the most devastating consequences for society. Strategically unimportant firms might get by with modest defenses, whereas robust defenses may be needed for critical industries.[267] Finally, what follows is by no means an exhaustive list of possible responses to cyber-insecurity. It is merely a list of responses suggested by conceiving of cyber-security in environmental, antitrust, products liability, and public health terms. Other solutions, suggested by other analytical frameworks, may be just as promising.

A. Monitoring and Surveillance

Effective cyber-security depends on the generation and exchange of information.[268] An ideal system would create and distribute vulnerability data (the holes intruders might exploit to gain access to computer systems), threat data (the types of malware circulating on the Internet and the types of attacks firms have suffered), and countermeasure data (steps that can be taken to prevent or combat infection by a particular piece of malicious code).[269] Perhaps the best way to collect this information is through a distributed surveillance network akin to the biosurveillance system at the heart of public health law. Companies are unlikely to participate in this sort of arrangement due to fears of liability under antitrust and other laws.[270] A suite of measures is therefore needed to help foster favorable incentives, including subsidies, threats of liability, and offers of immunity. These steps would not guarantee that firms will collect and share cyber-security data, but they would make such arrangements more viable than they are at present.

Public health law's system of distributed biosurveillance seems well suited to the challenge of gathering and disseminating cyber-security data. Like health care providers who diagnose and then report their patients' infectious diseases, firms could be tasked with monitoring their systems for vulnerabilities and intrusions, then reporting their findings and the countermeasures they have implemented to designated recipients.[271] Such a

---

[266] AM. BAR ASS'N, *supra* note 18, at 21; Katyal, *Criminal Law*, *supra* note 10, at 1080; Nojeim, *supra* note 14, at 119.

[267] *See supra* notes 61−66 and accompanying text.

[268] *But see* CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 45 (information sharing should not be "a primary goal").

[269] *See supra* notes 153−54 and accompanying text.

[270] *See supra* notes 155−68, 201−08 and accompanying text.

[271] Mulligan & Schneider, *supra* note 19, at 81.

system would take advantage of important information asymmetries. Individual companies often know more than outsiders about the vulnerabilities in their systems and the types of intrusions they have faced; they have a comparative advantage in compiling this data.[272] The principal alternative—surveillance by a single, central regulator—is unlikely to be as effective. As F.A. Hayek emphasized, "the knowledge of the [economic] circumstances of which we must make use never exists in concentrated or integrated form, but solely as the dispersed bits of incomplete and frequently contradictory knowledge which all the separate individuals possess."[273] The same is true of cyber-security data. A central regulator lacks the capacity to examine each device that is connected to the Internet to determine its vulnerabilities, and cannot inspect every data packet transiting the Internet to determine whether it contains malicious code. And even if the scope of the project was not prohibitively vast, the privacy costs associated with a central monitor—especially a government monitor—would likely be intolerable.[274] Instead, the better course would be to rely on individual firms to gather the relevant information.[275]

While firms would be responsible for the lion's share of monitoring, the government still has an important role to play: providing especially sensitive companies, such as power companies and ISPs, with information about especially sophisticated forms of malware. Here, the comparative advantage is reversed; the government's highly resourceful intelligence agencies are simply better than the private sector at detecting intrusions by sophisticated adversaries like foreign militaries and developing countermeasures.[276] The government can provide these firms with the signatures of malware used in previous attacks, and firms can use the signature files to detect future intrusions. In 2010 the National Security Agency began assisting Google in detecting intrusions into its systems. The partnership was announced in the wake of reports that sophisticated hackers, most likely affiliated with China's intelligence service, had broken into Google's systems and collected data about users, including a number of human rights activists.[277] The NSA reportedly has entered a similar partnership with a number of large banks.[278]

---

[272] *See* CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 53; Bamberger, *supra* note 210, at 391–92; Katyal, *Criminal Law*, *supra* note 10, at 1091. *See generally* Bamberger, *supra* note 210, at 399 (emphasizing "the information asymmetries between regulated firms and administrative agencies").

[273] F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 519 (1945).

[274] Mulligan & Schneider, *supra* note 19, at 81.

[275] *See* CLARKE & KNAKE, *supra* note 1, at 162.

[276] Coldebella & White, *supra* note 14; Condron, *supra* note 19, at 407. *But see* O'Neill, *supra* note 19, at 265, 275; Taipale, *supra* note 96, at 9.

[277] Nakashima, *Google*, *supra* note 58.

[278] Andrea Shalal-Esa & Jim Finkle, *National Security Agency Helps Banks Battle Hackers*, REUTERS (Oct. 26, 2011, 2:51 PM), http://www.reuters.com/article/2011/10/26/us-cybersecurity-banks-idUSTRE79P5E020111026.

At least two possibilities exist for how to structure the system used to disseminate the information compiled by private firms. Some commentators have called for a central repository of cyber-security data—a "cyber-CDC,"[279] as it were. Under such a system, an individual firm would notify the clearinghouse if it discovers a new vulnerability in its systems, or a new type of malicious code, or a particular countermeasure that is effective against a particular kind of threat. The repository would analyze the information, looking for broader trends in vulnerabilities and threats, then issue alerts and recommendations to other firms. This clearinghouse might be a government entity, as in public health law, but it need not be. An alternative architecture would be for firms to exchange cyber-security information with one another directly, on a peer-to-peer basis, rather than first routing it through a central storehouse. One advantage of the peer-to-peer approach is that it may be more resilient. A CDC-type clearinghouse would be an attractive target for cyber-adversaries, and the entire system would fail if it were compromised.

Distributed surveillance may be an even better fit for cyber-security than for public health, for several reasons. First, malicious computer code can often be detected more quickly than biological pathogens,[280] which means that countermeasures can be developed and put in place rapidly. Biosurveillance can be slow because the incubation period for certain diseases—the amount of time between when a disease is contracted and when its symptoms first manifest—can be days or weeks. By contrast, it is possible to detect known malware in real time, as the code is passing through a company's system. Of course, malware detection is imperfect.[281] Deep packet inspection and other forms of network monitoring typically work by comparing streams of data against signatures of known malicious code.[282] These systems are only as good as their underlying definitions files. If there is no signature for a particular type of malware, chances are it will not be detected. As a result, sophisticated "zero-day" attacks—so called because they occur before the first day on which security personnel become aware of them and begin to develop countermeasures—may well go unnoticed.[283] Former CIA director Jim Woolsey emphasizes that "[i]f you can't deal with a zero-day attack coming from a thumb drive . . . you have nothing."[284] Of course, these are the very sorts of attacks likely to be launched by sophisticated adversaries like foreign intelligence services. Public health law's biosurveillance framework thus is probably better at

[279] IBM, *supra* note 19, at 13–14; *see also* Sharp, *supra* note 8, at 25.

[280] Rattray et al., *supra* note 8, at 152.

[281] CLARKE & KNAKE, *supra* note 1, at 162; Sklerov, *supra* note 19, at 74.

[282] *See supra* note 163 and accompanying text.

[283] Rosenzweig, *supra* note 14, at 28 n.23; Zetter, *supra* note 48.

[284] MCAFEE & CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 15, at 1.

detecting intrusions of low to modest complexity than those undertaken by foreign governments.

Second, cyber-threat monitoring has the potential to raise fewer privacy concerns than biosurveillance.[285] Health care providers often give authorities sensitive information about individual patients, such as their names, Social Security numbers, and other personally identifiable information, as well as the diseases they have contracted.[286] A properly designed cyber-monitoring system need not compile and disseminate information of the same sensitivity. Collection and sharing could be limited to information about the incidence and prevalence of known malware. The fact that the "ILoveYou" worm has infected a particular system exposes a great deal less personal information, and thus raises weaker privacy concerns, than the fact that a particular patient suffers from HIV or breast cancer.

The challenge, then, is to provide firms with incentives to collect and disseminate cyber-security information.[287] At present companies have strong disincentives to do so, partly due to fears of legal liability,[288] but also because of concerns about compromising trade secrets, losing customer goodwill, and reputational harms.[289] Public health law facilitates collection and sharing through both direct regulation, such as state statutes requiring health care providers to notify authorities about patients who have contracted various infectious diseases, and less coercive alternatives.[290] A similar arrangement might be adopted for cyberspace. The government could require firms to gather information about the vulnerabilities in their systems, the types of attacks they have suffered, and the countermeasures they have used to combat malware, and then to disseminate the data to designated recipients.[291] Imposing such an obligation would not eliminate companies' incentives to withhold cyber-security data. It would simply make it more costly for them to do so, where costs include the sanctions for hoarding discounted by the probability of punishment. Firms will be more likely to collect and share cyber-security data, but some will still find it advantageous to hoard.

There is also a less coercive, and probably more effective, alternative. Cyber-security data is a sort of public good, and economic theory predicts

---

[285] *But see* Nojeim, *supra* note 14, at 126.

[286] *See* GOSTIN, *supra* note 221, at 297.

[287] Nojeim, *supra* note 14, at 128.

[288] *See supra* notes 155−68, 201–08 and accompanying text.

[289] *See, e.g.*, Aviram, *supra* note 79, at 154; Aviram & Tor, *supra* note 139, at 240; Bambauer, *Conundrum*, *supra* note 12, at 611; Katyal, *Digital Architecture*, *supra* note 15, at 2278; Nojeim, *supra* note 14; Powell, *supra* note 14, at 501; Rosenzweig, *supra* note 14, at 9. *But see* O'Neill, *supra* note 19, at 281 (arguing that intercompany cooperation against cyber-attacks is not altogether uncommon).

[290] *See supra* notes 235–42 and accompanying text.

[291] Frye, *supra* note 153, at 370–71.

that it will be underproduced.[292] Firms might be offered subsidies to encourage them to compile and exchange the needed information.[293] These bounties could be direct payments from the government, tax credits, or deductions. They could also take the form of enhanced intellectual property protections for the cyber-security information firms generate. If the subsidies are large enough, firms will have an incentive not just to report the data they have already compiled, but to invest in discovering previously unknown vulnerabilities, threats, and countermeasures.[294]

Antitrust law can also help recalibrate firms' incentives.[295] Antitrust is often skeptical of information sharing and other forms of cooperation among competitors.[296] But exchanges of cyber-security data can enhance consumer welfare by preventing attacks from taking place or at least mitigating their effects.[297] One way to incentivize companies to cooperate is to alleviate their apparently widespread fears of antitrust liability through judicial, administrative, or legislative action. Federal courts could expressly discard the per se approach and substitute a rule of reason when reviewing private sector agreements to share cyber-security data or to adopt common security protocols. Instead, arrangements would be judged on a case-by-case basis, and would stand or fall based on the degree to which they actually advance or hinder consumer welfare. This would reduce the risk of false positives—the danger that the coarse-grained per se rule might invalidate a cyber-security initiative that is actually welfare-enhancing. While this approach shows promise, it also carries some significant drawbacks. A judicial response may not sufficiently remove legal uncertainty. Companies will not always be able to predict whether reviewing courts will sustain or invalidate a proposed cyber-security venture, and the risk of liability will dissuade firms from forming them.[298] In short, the uncertain prospects of ex post judicial approval may not provide firms with enough assurance ex ante.

A more promising approach would be for administrative agencies to sponsor cyber-security exchanges, as some in Congress have proposed.[299] Agencies with special expertise in cyber-security (such as the NSA and the Department of Homeland Security) could partner with the agencies that are

---

[292] *See supra* notes 137–39 and accompanying text. *But see* Aviram & Tor, *supra* note 139, at 240–47 (arguing that information can be a rivalrous good).

[293] *See* Nojeim, *supra* note 14, at 128.

[294] *But see* Malloy, *supra* note 86, at 572–73 (predicting that firms will tend to neglect "regulatory investments"—i.e., expending scarce resources to obtain benefits offered to those who comply with government regulations).

[295] *Cf.* Adler, *supra* note 155 (discussing antitrust law in the context of marine resources, another public good).

[296] *See supra* notes 235–42 and accompanying text.

[297] *See supra* notes 153–54 and accompanying text.

[298] *See supra* notes 165–68 and accompanying text.

[299] *See* Cybersecurity Act of 2012, S. 2105, 112th Cong. § 301 (2012).

responsible for enforcing federal antitrust laws (the Federal Trade Commission and the Justice Department's antitrust division) to establish fora in which companies could establish common security standards and exchange information. The government's participation in these fora would offer assurances that they are being used for legitimate purposes and not as vehicles for anticompetitive conduct. From the standpoint of participating firms, this approach is advantageous because it offers them de facto antitrust immunity.[300] It is unlikely that an agency such as the FTC or DOJ that sponsored a cooperative cyber-security arrangement later would go to court to have it invalidated. And while the blessing of these agencies does not formally bind other potential plaintiffs, such as state attorneys general or private parties, their determination that a proposed venture is permissible under federal antitrust laws probably would receive a healthy dose of judicial deference. Government sponsorship has another advantage: it can help solve the coordination and free-rider problems associated with collective action.[301] A regulator can mitigate these tendencies by coercing firms into participating in the forum and complying with its requirements; it also can withhold the forum's benefits from firms that shirk.

A third alternative would be for Congress to enact a cyber-security exception to the antitrust laws.[302] The upside of a legislative carve-out is that it would eliminate virtually all risk of liability and thus remove one powerful disincentive for companies to cooperate on cyber-security initiatives. Ideally, such a measure would be narrowly tailored to the precise sort of interfirm cooperation that is desired—the exchange of vulnerability, threat, and countermeasure information and the development of common security protocols. In other words, the exemption would be pegged to specific conduct, and would not immunize entire industries (as used to be the case with major league baseball[303]). A broader exception would offer few additional cyber-security gains and could open the door to anticompetitive conduct.

We also might consult products liability law for ideas on how to incentivize companies to exchange cyber-security data. Firms do not have strong incentives to search for vulnerabilities in their systems or products, and ISPs are reluctant to monitor network traffic for malicious code.[304] Lawmakers might use a combination of carrots and sticks to recalibrate these incentives. Offers of immunity would increase companies' expected

---

[300] BRENNER, *supra* note 1, at 228.

[301] *See* Kobayashi, *supra* note 136, at 23.

[302] Katyal, *Community*, *supra* note 135, at 52.

[303] *See* Flood v. Kuhn, 407 U.S. 258 (1972), *superseded by statute*, 15 U.S.C. § 26b (2006); Fed. Baseball Club of Balt., Inc. v. Nat'l League of Prof'l Baseball Clubs, 259 U.S. 200 (1922).

[304] *See supra* notes 201–08 and accompanying text.

benefits of compiling and sharing cyber-security data; threats of liability would increase their expected costs of failing to do so.[305]

Consider the carrots first. Firms could be offered immunity from various laws that presently inhibit them from collecting and exchanging certain information about cyber-vulnerabilities and threats. In particular, Congress could expand the service-provider exception to the Federal Wiretap Act's general ban on intercepting electronic communications.[306] And the exception could be broadened to authorize ISPs to monitor network traffic for malicious code that threatens their subscribers' systems, not just their own. Congress could also authorize ISPs to notify customers whose systems are found to be infected by malware.[307] It further could expressly preempt any state laws to the contrary. This would foreclose any claims that monitoring for malware violates state privacy law or breaches the terms of service between an ISP and its subscribers. In all cases, eligibility for these forms of immunity could be conditioned on information sharing: a company would not be able to take advantage of the safe harbor unless it shared the information it discovered with other firms. The result would be to foster strong incentives to exchange data about threats and vulnerabilities.

As for the sticks, below I propose modifying tort law's traditional economic loss doctrine in the cyber-security context.[308] Firms that implement approved security standards would enjoy immunity from lawsuits seeking redress for injuries sustained from an intrusion; companies that disregard the protocols would be subject to lawsuits for any resulting damages. Under such a scheme, a company that implemented the standards might have its immunity stripped if it failed to share information about known weaknesses in its systems or products. As for firms that fail to adopt the security standards, the lack of information sharing could be treated as an aggravating factor; extra damages could be imposed on firms that are aware of vulnerabilities or threats but fail to share that information with other companies. This series of tiered penalties would produce marginal deterrence; firms would have good reason not only to implement the approved security standards, but also to exchange the threat and vulnerability information on which those protocols depend.

B. Hardening Targets

A second objective for a cyber-security regime is to harden critical systems against attack by developing effective security protocols.[309] The

[305] Malloy, *supra* note 86, at 531–32. *But see id.* at 572–73 (predicting that firms will tend to neglect "regulatory investments"—i.e., complying with regulations to receive the benefits they offer).

[306] *See* 18 U.S.C. § 2511(2)(a)(i) (2006).

[307] BRENNER, *supra* note 1, at 229–31; CLARKE & KNAKE, *supra* note 1, at 164–65.

[308] *See infra* notes 339–44 and accompanying text.

[309] CLARKE & KNAKE, *supra* note 1, at 159.

goal of such measures is to prevent cyber-intruders from harming these systems at all, as opposed to limiting the amount of damage intrusions can do; the objective is to increase impregnability as opposed to their survivability.[310] Of course, some cyber-attacks inevitably will succeed, so enhancing survivability, as discussed below,[311] is an essential goal as well. The regulatory disciplines surveyed above suggest various techniques for encouraging companies to adequately secure their networks. Environmental law suggests the need for industry-wide security standards; these rules should be developed through collaborative partnerships between regulatory agencies and private firms, rather than imposed via direct regulation. Products liability law suggests that pairing threats of liability with offers of immunity can incentivize firms to implement the security standards. And public health law's use of mandatory vaccinations might be adapted by incentivizing firms to take certain minimum steps to secure their systems. Again, different firms and industries face different vulnerabilities, threats, and consequences, so the resulting security standards should be calibrated to the particular conditions in individual industries.

Regulators could improve critical systems' defenses by establishing and enforcing new cyber-security protocols akin to the environmental regulations that restrict, say, the amount of sulfur dioxide a given source may emit into the atmosphere.[312] Regulatory standards can help manage the negative externalities that result when a company suffers a cyber-intrusion. It should be emphasized at the outset that the specific content of any cyber-security standards is well beyond the scope of this Article.[313] My focus here

---

[310] *See supra* note 260 and accompanying text.

[311] *See infra* Part III.C.

[312] It is also possible to develop new cyber-security standards through litigation. *See* Harper, *supra* note 127; Johnson, *supra* note 217, at 275–76; Rosenzweig, *supra* note 14, at 23. A court might hold, for instance, that a given firm's failure to adopt a particular security measure breaches a general duty of care. This option seems less promising than the regulatory approach for several reasons. First, courts may not have the technical expertise to fashion detailed security protocols for complicated systems and products. Second, there is the problem of legal uncertainty. A regulation is likely to be more determinate than a series of incremental judicial opinions, especially in the context of a highly complex subject matter like cyber-security; relying on litigation thus runs the risk that firms will not know what is expected of them. There is, of course, an important role for litigation—the prospect of civil liability creates incentives for firms to comply with the regulatory standards. *See infra* notes 339–51 and accompanying text. But litigation should be limited to enforcing the standards, not formulating them in the first place.

[313] Just within the legal literature—to say nothing of computer science, economics, and other fields—authors have debated relatively modest regulations, such as mandating that firms use encryption, firewalls, and intrusion-detection systems, Condron, *supra* note 19, at 410; Gable, *supra* note 2, at 94–95, requiring companies that operate certain sensitive systems to authenticate users before granting them access, Nojeim, *supra* note 14, at 131–33; Sklerov, *supra* note 19, at 22–24, and disconnecting vulnerable SCADA systems from the Internet, *see* CLARKE & KNAKE, *supra* note 1, at 167–69; MCAFEE, *supra* note 37, at 34. Others have debated even more dramatic proposals, such as requiring ISPs to monitor the traffic that flows over their networks for malicious code, Katyal, *Criminal Law*, *supra* note 10, at 1007, 1095–101; Lichtman & Posner, *supra* note 61, at 222; Taipale, *supra* note

is not on the technical feasibility or policy advantages of any particular defensive measure. Instead, the focus of this Article is establishing regulatory mechanisms by which new cyber-security standards—whatever their content—may be adopted.

Turning to that question, one obvious option would be for administrative agencies to use traditional "command and control" regulation—to issue a set of mandatory standards and incentivize firms to comply with them by threatening civil or criminal penalties.[314] This is a fairly common approach in environmental law,[315] and some scholars have urged the government to adopt it here. Neal Katyal argues that "direct government regulation" of cyber-security "is the best solution," and calls for regulatory agencies to issue "the equivalent of building codes to require proper design and performance standards for software."[316] Likewise, a prominent think tank argues that "the federal government bears primary responsibility" for cyber-security and that "it is completely inadequate" to leave the matter "to the private sector and the market."[317] Some have even called for the federal government to take over certain sectors of the economy in the name of cyber-security. According to an ABA task force, "government may also need to 'semi-nationalize' some sectors (like the electricity grid) where isolation is not an option and the adverse consequences of certain low probability events are likely to be very high."[318] It isn't steel mills, but Harry Truman would have admired the proposal.[319]

Traditional command-and-control regulation seems ill suited to the task of securing the nation's cyber-infrastructure. The better course would be to involve the firms that operate these assets in establishing and implementing new security protocols. Private sector participation—an approach sometimes seen in environmental law—is desirable for several familiar reasons. First, information asymmetries: companies often know more than regulators about the vulnerabilities in their systems, the types of

96, at 34, or moving to an entirely new Internet architecture (such as IPv6) in which anonymity is reduced and user activity is capable of being traced. BAKER, *supra* note 24, at 231–32; LESSIG, *supra* note 67, at 45, 54; POST, *supra* note 94, at 84; Bambauer, *Conundrum*, *supra* note 12, at 590, 601; Frye, *supra* note 153, at 354; Katyal, *Digital Architecture*, *supra* note 15, at 2269–70; Taipale, *supra* note 96, at 31.

[314] Malloy, *supra* note 86, at 531.

[315] *See, e.g.*, Clean Water Act, 33 U.S.C. § 1319(b)–(c) (2006) (providing civil and criminal penalties); Clean Air Act, 42 U.S.C. § 7413(b) (2006) (providing civil penalties).

[316] Katyal, *Digital Architecture*, *supra* note 15, at 2284, 2286. *But see* Katyal, *Criminal Law*, *supra* note 10, at 1091 ("[Cyber-security regulation] places law enforcement in uncharted territory. It cannot know what the best, or cheapest, form of protection is . . . .").

[317] CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 15 (deeming cyber-security a matter of national security); *see also* Frye, *supra* note 153, at 376.

[318] AM. BAR ASS'N, *supra* note 18, at 27.

[319] *See generally* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

intrusions they have faced, and the most effective countermeasures for dealing with those threats.[320] Second, a related concern is that regulators probably lack the knowledge necessary to determine the socially optimal level of cyber-breaches and set the security standards accordingly.[321] The market, through the price system, is capable of aggregating and processing this information in a way that central planners cannot. Third, rapid technological change makes it difficult for regulators to formulate durable security rules.[322] Vulnerabilities, threats, and countermeasures are in a constant state of flux, and regulatory standards cannot keep pace with these developments. Notice-and-comment rulemaking rarely takes less than two years, sometimes much longer,[323] and the rules likely would be obsolete before the ink in the *Federal Register* was dry. Fourth, there is a risk that government protocols will stifle innovation.[324] If regulatory agencies promulgate a set of mandatory standards, regulated firms will have less reason to search for newer and more efficient countermeasures; they will simply implement the government's directives.

What specific role should private firms have in developing and implementing cyber-security standards? At least two possibilities come to mind. First, regulators could practice a form of "delegated regulation"[325] in which they mandate broad security goals and establish the penalties for falling short, then leave it up to companies to achieve those goals in whatever manner they deem most effective.[326] Regulation by delegation is said to be appropriate where administrative agencies have the capacity to "identify specific outcomes but cannot easily codify in generally-applicable rules the means for achieving them."[327] Environmental law sometimes follows this approach, as do other fields such as food safety[328] and

---

[320] *See supra* notes 272–75 and accompanying text.

[321] Coyne & Leeson, *supra* note 14, at 488–89; Powell, *supra* note 14, at 502, 505.

[322] *See* BAKER, *supra* note 24, at 235, 237; CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 51; Rosenzweig, *supra* note 14, at 10.

[323] *See* William F. West, *Formal Procedures, Informal Processes, Accountability, and Responsiveness in Bureaucratic Policy Making: An Institutional Policy Analysis*, 64 PUB. ADMIN. REV. 66, 66, 69 (2004) (finding after studying the development of forty-two regulatory rules that the average time period between initiation of research and promulgation of a proposed rule was 4.3 years and the average length of comment taking was 5.3 years). In calculating the average length of comment taking, West excluded seven rules that either had open-ended notice-and-comment periods or were routine rules issued annually or under a statutory deadline. The average length of comment taking for these rules was still 2.2 years. *Id.*

[324] CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 51; Kobayashi, *supra* note 136, at 26.

[325] Schwartz & Janger, *supra* note 61, at 919; *accord* Bamberger, *supra* note 210, at 386; Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 551 (2000).

[326] Bamberger, *supra* note 210, at 380–81; *accord* AM. BAR ASS'N, *supra* note 18, at 9; CLARKE & KNAKE, *supra* note 1, at 134; Jensen, *Cyber Warfare*, *supra* note 15, at 1565.

[327] Bamberger, *supra* note 210, at 389.

[328] Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, 37 LAW & SOC'Y REV. 691, 696–98 (2003).

securities regulation.[329] For instance, the EPA's acid rain program affords companies a measure of discretion in deciding how to comply with their obligation under the Clean Air Act to reduce various emissions. And the EPA's "bubble" approach to the Clean Air Act allowed polluters to offset increased emissions from one source with decreased emissions from other sources, providing them with an incentive to experiment with new technologies that could reduce emissions at lower cost.[330] (Note that both programs involve discretion in implementing numerical values rather than, as would be true in the cyber context, substantive standards.) Delegated regulation seems a good fit for cyber-security, though not a perfect one. Giving companies discretion to implement the government's security standards achieves three of the four benefits of private action mentioned above: it avoids some problems with information asymmetries, allows for flexibility in reacting to fast-changing technologies, and promotes rather than stifles private sector innovation. However, difficulties would remain with formulating the standards. Regulators probably lack the knowledge needed to determine the socially optimal level of cyber-breaches and set the security standards accordingly.

An alternative would be a form of "enforced self-regulation"[331] in which private companies develop new cyber-security protocols in tandem with the government.[332] These requirements would not be handed down by administrative agencies, but rather would be developed through a collaborative partnership in which both regulators and regulated would play a role. In particular, firms might prepare sets of industry-wide security standards. The National Industrial Recovery Act, famously invalidated by the Supreme Court in 1935 on nondelegation grounds, contained such a mechanism,[333] and today the energy sector develops reliability standards in the same way.[334] Or agencies could sponsor something like a negotiated rulemaking in which regulators, firms, and other stakeholders forge a consensus on new security protocols.[335] In either case, agencies would then ensure compliance through standard administrative techniques like audits, investigations, and enforcement actions.[336] This approach would achieve all four of the benefits of private action mentioned above: it avoids some

[329] Bamberger, *supra* note 210, at 390–91.

[330] Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 839–40 (1984); *see also* Malloy, *supra* note 86, at 536, 541, 547–49 (discussing conflicting accounts of whether the bubble approach actually promoted innovation).

[331] Bamberger, *supra* note 210, at 461 (citing IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 101–32 (1995)).

[332] AM. BAR ASS'N, *supra* note 18, at 9; Coldebella & White, *supra* note 14, at 241–42; Katyal, *Criminal Law*, *supra* note 10, at 1099.

[333] A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495, 542 (1935).

[334] *See* CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 52–53.

[335] *See* 5 U.S.C. §§ 561–70 (2006).

[336] CTR. FOR STRATEGIC & INT'L STUDIES, *supra* note 8, at 52.

problems with information asymmetries, takes advantage of distributed private sector knowledge about vulnerabilities and threats, accommodates rapid technological change, and promotes innovation. On the other hand, allowing firms to help set the standards that will be enforced against them may increase the risk of regulatory capture—the danger that agencies will come to promote the interests of the companies they regulate instead of the public's interests.[337] The risk of capture is always present in regulatory action, but it is probably even more acute when regulated entities are expressly invited to the decisionmaking table.[338]

Products liability law likewise offers several strategies for hardening critical infrastructure against cyber-attacks. The prospect that a company might be required to pay money damages to those who have been injured by an attack on their systems or products would internalize costs that are now externalized onto others. Liability thus would incentivize firms to offer goods (such as computer software) and services (such as online banking) that are more secure.[339] Thanks to the economic loss doctrine, companies presently face little risk of liability for the injuries that result from their failure to prevent cyber-intrusions.[340] Modifying this default rule of de facto immunity could help foster incentives for firms to improve their cyber-defenses.

What could a recalibrated liability regime for cyber-security look like? Again, a combination of carrots and sticks could be used. Congress might abolish the economic loss doctrine for injuries that result from a given company's wrongful failure to prevent a cyber-attack. In its place, lawmakers could substitute a regime that imposes liability or offers immunity based on what steps a company has taken to secure its products or systems. As for the carrots, firms that implement the security standards that are developed in tandem with regulators, but nevertheless suffer cyber-

---

[337] *See generally* George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3 (1971) (arguing that industries seek out regulation in a manner that is designed and operated to primarily benefit the industry). A related problem is that, because of information asymmetries, agencies often depend on the companies they regulate to provide the data they need to formulate rules. Yet firms will have an incentive to underestimate vulnerabilities and threats to persuade regulators to approve lenient and less costly security protocols. Coyne & Leeson, *supra* note 14, at 489. Of course, that concern is also present in traditional regulation. There are also doctrinal difficulties. Depending on how the public–private partnership is structured, it conceivably could violate what remains of the nondelegation doctrine. *See, e.g.*, Carter v. Carter Coal Co., 298 U.S. 238, 310–12 (1936) (striking down a statute that authorized coal producers to establish minimum prices in certain geographic regions on the ground that it was an unconstitutional delegation of legislative power to private companies).

[338] USA Grp. Loan Servs., Inc. v. Riley, 82 F.3d 708, 714 (7th Cir. 1996) (Posner, C.J.) (describing negotiated rulemaking as "an abdication of regulatory authority to the regulated, the full burgeoning of the interest-group state, and the final confirmation of the 'capture' theory of administrative regulation").

[339] *See* Coyne & Leeson, *supra* note 14, at 492; Hunker, *supra* note 19, at 211; Johnson, *supra* note 217, at 260; Lichtman & Posner, *supra* note 61, at 232–39; Yang & Hoffstadt, *supra* note 15, at 207–10; Rosenzweig, *supra* note 14, at 23; Schneier, *supra* note 35.

[340] *See supra* notes 190–93 and accompanying text.

attacks, could be offered immunity from lawsuits seeking redress for the resulting damages.[341] This cyber "safe harbor" could extend not just to purely economic injuries (for which firms currently enjoy de facto immunity) but also to physical injuries and the associated economic harms (for which firms presently may be held liable). The scope of immunity thus would be broader than under current law, but it would only be available to companies that take the desired steps to improve their cyber-defenses. Lawmakers might use the Safety Act as a model.[342] The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 grants immunity to firms that sell certain antiterrorism goods and services, so long as they comply with various standards, including a requirement that they carry liability insurance.[343]

As for the sticks, firms that fail to implement the agreed security measures and then suffer cyber-attacks could be held liable for the full range of injuries that result from the intrusions. The severity of the damages could be pegged to the severity of their misconduct, thereby achieving marginal deterrence. A company that fails to adopt the approved security standards might be made to pay compensatory damages or even a smaller fixed sum set by statute, but a company whose conduct is more egregious—one that fails to share information about known vulnerabilities or threats, for instance—might be eligible for exemplary damages. For inspiration, lawmakers might look to the Gramm–Leach–Bliley Act, which imposes liability on banks that fail to protect consumer data,[344] contributing to the financial services sector's relatively robust defenses against cyber-intrusions.[345] Such a liability regime would increase both a firm's expected benefits of implementing the security protocols, as well as the expected costs of defying them.

Civil liability would also help promote a more robust market for cyber-security insurance. Insurers can have a profound effect on the steps firms take to secure their systems and products against cyber-intrusions, because they can insist that companies implement various security measures as a condition of coverage or charge higher premiums to those that do not.[346] Insurance companies provide a sort of second-order regulation, enforcing cyber-security standards by refusing to bear the losses of firms with poor records or engaging in price discrimination against them. The result is to provide the insured with financial incentives to implement the defenses their insurers are calling for. These incentives have

[341] *See* Coldebella & White, *supra* note 14, at 235.

[342] BAKER, *supra* note 24, at 234–35.

[343] 6 U.S.C. §§ 441–44 (2006).

[344] 15 U.S.C. § 6801(b) (2006); *see supra* notes 209–10 and accompanying text.

[345] *See supra* notes 213–17 and accompanying text.

[346] *See* BRENNER, *supra* note 1, at 225; Bamberger, *supra* note 210, at 456; Coyne & Leeson, *supra* note 14, at 491–92; Rosenzweig, *supra* note 14, at 23–24.

already borne fruit. According to Bruce Schneier, "[f]irewalls are ubiquitous because auditors started demanding firewalls. This changed the cost equation for businesses. The cost of adding a firewall was expense and user annoyance, but the cost of not having a firewall was failing an audit."[347] Enforcement by insurers also can decrease the government's enforcement costs; there is less need for regulators to verify that firms are complying with the agreed security standards if insurers, pursuing their own financial interests, are already doing so.

At present, the market for cyber-security insurance is fairly underdeveloped (though some insurance companies have begun to offer coverage[348]), in part because firms currently face very little risk of liability for injuries resulting from cyber-attacks on their systems or products; why insure when one is effectively immune?[349] The prospect of civil liability is a critical first step in creating a viable market for cyber-security insurance.[350] Lawmakers might further stimulate the market by offering various kinds of subsidies. For instance, the government might provide insurers with more information (including, perhaps, classified information) about the incidence, prevalence, and consequences of various sorts of malicious code. Insurers could use this data to more accurately assess the probability of cyber-intrusions and their potential costs, which would help in setting premiums.[351] Or the government might offer tax benefits to insurers that offer cyber-security policies. Or it might require certain companies, such as strategically important firms like public utilities or companies that supply goods or services to the government, to carry cyber-security insurance.

Public health law suggests a final approach to hardening critical infrastructure. Most states have enacted laws requiring schoolchildren to be vaccinated against various diseases,[352] and lawmakers might adopt similar measures for cyberspace. In both contexts, compulsory inoculation helps reduce negative externalities and foster positive ones. Just as an unvaccinated child might infect classmates with a pathogen, a computer system that lacks effective cyber-defenses might be commandeered into a botnet. In addition, a child who has been vaccinated contributes to herd immunity and thereby decreases the probability that other, unvaccinated students will contract the disease. In the same way, companies that adopt

---

[347] Schneier, *supra* note 35, at 1.

[348] Coyne & Leeson, *supra* note 14, at 491; Yang & Hoffstadt, *supra* note 15, at 208–09.

[349] AM. BAR ASS'N, *supra* note 18; BRENNER, *supra* note 1, at 225. Another challenge is that it is difficult for insurers to write policies when—as is often the case with cyber-attacks—the probability and consequences of an incident are uncertain. *See, e.g.*, Michelle Boardman, *Known Unknowns: The Illusion of Terrorism Insurance*, 93 GEO. L.J. 783, 784 (2005) (arguing that insurance coverage for international terrorism is not possible without adequate actuarial data to calculate risk levels).

[350] Rosenzweig, *supra* note 14, at 23.

[351] Coyne & Leeson, *supra* note 14, at 491–92; Frye, *supra* note 153, at 366–67.

[352] *See supra* note 229 and accompanying text.

effective cyber-defenses make it less likely that their systems will be used to transmit malware to other users.

What would mandatory vaccination look like in cyberspace? Several variants exist. The most coercive approaches involve direct regulation, akin to a requirement that all citizens receive a particular vaccine. One option would be for lawmakers to mandate that every computer user (or, less dramatically, firms in particularly sensitive industries such as the telecommunications sector) install certain security products on their systems, such as antivirus software or firewalls. Think of it as a digital equivalent of the Patient Protection and Affordable Care Act's "individual mandate" to purchase health insurance.[353] An alternative would be for the government to require ISPs to provide their customers with a specified security software package.[354] ISPs presumably would pass on the costs of the software to their subscribers, so the effect would be the same as the individual mandate approach—users would be made to pay a premium for a security product they previously declined to purchase. Or, the government could compensate the ISPs for the costs of making the security package available to their subscribers. In that event, the scheme would represent a (likely regressive) wealth transfer from taxpayers who do not use computers to those who do.

Another less coercive set of options would withhold or offer certain benefits to incentivize security improvements; they are the equivalent of making vaccination a condition of eligibility to attend public schools. The ability to access the Internet, as opposed to local or proprietary networks, is a valuable benefit of the service one receives from an ISP—for many subscribers it is the most valuable benefit ISPs offer—and it might be conditioned on a subscriber taking steps to improve cyber-security. In particular, regulators could direct ISPs to refuse to route users' traffic to the public Internet unless they are able to verify that the users have installed specified security software on their systems.[355] Alternatively, government web sites could refuse any traffic sent from a system that has not adopted specified security measures. Users thus would be unable to, for example, post comments in an online rulemaking docket or check the status of a tax refund unless they adopted the security measures. This sort of measure depends on the ability to authenticate the identity of the sender, as well as the presence of various cyber-defenses on its system. That capability does not presently exist, because the TCP/IP routing protocol is unconcerned with the sender's identity,[356] though some scholars believe an authenticated Internet is inevitable.[357] Finally, the government could offer tax credits or

[353] 26 U.S.C.A. § 5000A(a) (West 2010).

[354] *See* CLARKE & KNAKE, *supra* note 1, at 165; Sharp, *supra* note 8, at 25.

[355] *See* Rattray et al., *supra* note 8, at 160.

[356] *See supra* notes 118–20 and accompanying text.

[357] *See* BAKER, *supra* note 24, at 231–32; LESSIG, *supra* note 67, at 45.

deductions to firms or individual users that install the specified security software on their systems—another (likely regressive) wealth transfer.

C. Survivability and Recovery

The third thing an ideal cyber-security regime would do is promote resilience, thus limiting the amount of damage attackers can do to critical infrastructure. Here, the goals are survivability and recovery, not impregnability.[358] As Derek Bambauer emphasizes, "[m]itigation, not prevention, is the key."[359] The need to build resilience into the nation's cyber-defenses is a concession to reality; no matter how good one's defenses are, some attackers will be able to breach them. As a result, it is not enough to try to prevent attacks altogether. It is also necessary to minimize the amount of harm that the inevitably successful intrusions can do, and to restore victims to the status quo ante as quickly as possible.

Public health law offers several strategies for improving resilience. In realspace, quarantine and isolation aim at minimizing the harm a pathogen can do; once an outbreak is underway, we want to contain the disease and limit the number of people to whom it can spread. Quarantine and isolation might be adapted for cyberspace—where the goal is to prevent malicious code from infecting more machines—in any number of ways. The most straightforward approach would be for authorities, in the event of a cyber-attack, to order systems that are known or suspected to be infected with malware to temporarily disconnect from the Internet. While in quarantine, the systems could be inspected to see if they are in fact carrying malicious code. If not, they could be reconnected; if so, they could be repaired. The analogy to public health law is fairly exact: separation of the infected, whether physical or virtual, prevents them from spreading the contagion to others and presents an opportunity for treatment. While potentially effective, this approach has a significant drawback—legitimate users will be unable to access the infected system while it is offline. Putting a bank into cyber-quarantine does not just keep hackers from stealing money, it also keeps a customer from logging on to pay a credit card bill. A less drastic way of preventing the spread of malware would be to isolate *traffic* rather than *systems*. Infected systems would remain connected to the Internet, but authorities could use or require firms to use deep packet inspection to determine if the data the systems are sending and receiving contain malware. If a given packet is found to be carrying malicious code, it could be blocked; if not, it would be allowed to continue on its way. The public health analogy is allowing a man infected with SARS to leave an isolation facility and go about his business while wearing a surgical mask that intercepts the respiratory droplets through which the virus is spread. The virtue of this finer-grained variant is that it allows legitimate users to

[358] *See supra* note 260 and accompanying text.

[359] Bambauer, *Ghost*, *supra* note 25, at 5.

continue to access an infected system even as attackers are prevented from using it for their malign purposes; the hackers are thwarted, but customers can still access their accounts, although perhaps a bit more slowly than usual. On the other hand, traffic quarantines will only be as effective as the packet sniffers and malware signature files on which they rely, and sophisticated adversaries might be able to defeat both.

Another more controversial set of options involves preventive quarantine—separating systems that have not been infected but that are vulnerable. This approach would turn public health law on its head: rather than isolating the sick, authorities would isolate the healthy. The most aggressive variant would require a select group of strategically significant firms, such as the power grid, financial institutions, and telecommunications carriers, to temporarily disconnect from the Internet if a cyber-attack takes place.[360] Senator Nelson Rockefeller introduced legislation along these lines in 2009,[361] but critics denounced it as an "Internet Kill Switch."[362] Preventive quarantine would be a fairly effective way of preventing malware from spreading to critical infrastructure because a system that isn't on the Internet can't contract a virus that spreads online. But it wouldn't be infallible. Even "air gapped" systems—those that are physically separated from the Internet[363]—are vulnerable to infection via USB devices and other removable media.[364] A disconnection requirement could also prove quite costly: the affected systems would be unavailable to legitimate users for as long as the order remained in effect. There is also a risk that regulators might pull the disconnection trigger too readily. As an alternative to a strict disconnection requirement, regulators might direct strategically significant firms to implement security countermeasures of their own devising in the event of a cyber-attack. Senator Joseph Lieberman introduced legislation along these lines in 2010,[365] and it likewise was denounced as a kill switch.[366] Whatever the content of these security protocols—encrypting data to prevent its theft, for

[360] *Cf.* BRENNER, *supra* note 1, at 234 (recommending efforts to "restrain the connection of the electricity grid to public networks"); CLARKE & KNAKE, *supra* note 1, at 167 (proposing that federal regulators "focus[] on disconnecting the control network for the power generation and distribution companies from the Internet"); Picker, *supra* note 44, at 126–27 (arguing that critical infrastructure should be isolated from public networks as a means to lessen the impact of cyber-terrorism).

[361] Cybersecurity Act of 2009, S. 773, 111th Cong. (2009).

[362] *See, e.g.*, Mark Gibbs, *The Internet Kill Switch*, NETWORK WORLD, Apr. 13, 2009, at 34.

[363] BRENNER, *supra* note 1, at 84; Ellen Nakashima, *A Cyberspy Is Halted, but Not a Debate*, WASH. POST, Dec. 9, 2011, at A1, *available at* http://articles.washingtonpost.com/2011-12-08/national/35287794_1_malware-computer-network-military-operations.

[364] *See* BAKER, *supra* note 24, at 216; BRENNER, *supra* note 1, at 61; CLARKE & KNAKE, *supra* note 1, at 127; Baker, *supra* note 29; Nakashima, *Cyberspy*, *supra* note 363.

[365] Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010).

[366] *See e.g.*, Adam Cohen, *What's Missing in the Internet Kill-Switch Debate*, TIME (Aug. 11, 2010), http://www.time.com/time/nation/article/0,8599,2009758,00.html.

instance, or requiring users to authenticate themselves before gaining access to the system—they could be established through the collaborative regulatory partnership described above.[367] An even more modest version of preventive quarantine would be, as above, to segregate traffic rather than entire systems. In the event of a cyber-attack, packet sniffers might be used to inspect all traffic that is sent to and from designated systems. This would allow the systems to continue to operate more or less as usual, though perhaps at a cost of less security.

Another important goal is to ensure that critical systems are able to continue functioning during a cyber-attack and recover quickly thereafter. One way to achieve this is to build systems with excess capacity—to include more capabilities than a firm needs for its day-to-day operations, which can be held in reserve and called into service if an attack takes place.[368] In particular, regulators might require certain companies to build their systems with excess bandwidth. A "strategic reserve of bandwidth" is an especially useful countermeasure for defending against denial-of-service attacks;[369] if a company's servers are being overwhelmed, the reserve bandwidth can be brought into service to process the requests. Regulators also might require certain companies to maintain redundant data storage capabilities. These firms might routinely back up their data to servers that are dispersed both geographically and in network terms. If a cyber-attack corrupted their systems, it would be relatively easy to wipe them clean and restore the data from an uncorrupted backup.[370] An attacker thus might succeed in taking down one site "only to find that the same content continues to appear through other servers. This is like playing electronic Whac-A-Mole on a global scale . . . ."[371] These sorts of measures are akin to the public health practice of stockpiling medicines and vaccines for use in a crisis. The CDC may not need 300 million doses of smallpox vaccine in its everyday operations, but they would prove critical in the event of an outbreak.

Excess capacity can be expensive; requiring firms to keep reserves of largely unused bandwidth costs money, and "[h]aving information located in multiple places makes it more costly to maintain."[372] One way to pay for these measures would be for companies to pass their costs of complying with resilience mandates to their customers in the form of price increases, service decreases, or both. A difficulty with this approach is that improving a given company's ability to withstand an attack does not just confer benefits on its customers. It also confers benefits on third parties; if

---

[367] *See supra* Part III.B.

[368] *See* Benkler, *supra* note 260, at 75.

[369] Taipale, *supra* note 96, at 37.

[370] *See* Bambauer, *Conundrum*, *supra* note 12, at 637; Taipale, *supra* note 96, at 38.

[371] BRENNER, *supra* note 1, at 179.

[372] Bambauer, *Conundrum*, *supra* note 12, at 637.

Citibank can continue to operate notwithstanding a DDOS, its customers will still be able to pay their bills, and third-party vendors will still be able to receive payments. Excess capacity thus creates positive externalities, and the customers who pay higher prices for excess capacity are effectively subsidizing others. Another option would be for the government to offer various subsidies to firms that are subject to survivability mandates. This approach is based on a recognition that excess capacity is, in a sense, a public good that the market will tend to undersupply.[373] In part because excess capacity requirements can be costly, regulators would only apply them to selected firms of special strategic significance.

D. Responding to Cyber-attacks

The fourth and final component of an effective cyber-security regime is responding to individuals, groups, and states that have committed cyber-attacks. This topic naturally lends itself to analysis under the law enforcement and armed conflict frameworks, and it is exhaustively covered in the existing literature.[374] For instance, scholars have proposed better international cooperation on cyber-crime investigations, increasing the penalties for certain computer-related offenses, increasing the costs that perpetrators must bear to commit cyber-crimes, treating intrusions as "armed attacks" that trigger the right to self-defense under the United Nations Charter, treating cyber-attacks as acts of aggression that justify retaliating with conventional military force, and so on.[375] This Article does not seek to add to this already voluminous literature. There is, however, one type of response that deserves brief mention: active self-defense, or "hackbacks."

A hackback is an in-kind response to a cyber-attack. The victim essentially mounts a counterattack against the assailant, "shutting down the attack before it can do further harm and/or damaging the perpetrator's system to stop it from launching future attacks."[376] This might be accomplished in several ways. If a victim detects that it is experiencing a cyber-attack, it might direct a flood of traffic to the servers through which the attack is being routed, temporarily overwhelming them and preventing them from continuing the intrusion.[377] Or it might hack into the responsible servers, taking control of them or damaging them.[378] Some scholars believe

[373] *See supra* notes 137–44 and accompanying text.

[374] *See* sources cited *supra* note 19.

[375] *See supra* Part II.A.

[376] Sklerov, *supra* note 19, at 25; *see also* Condron, *supra* note 19, at 410–11; O'Neill, *supra* note 19, at 280.

[377] Condron, *supra* note 19, at 410–11.

[378] Smith, *supra* note 17, at 177–78.

that hackbacks are the most effective defense against cyber-attacks,[379] in part because active self-defense can avoid the attribution problem; a victim firm that is experiencing an intrusion could retaliate against any computer that is attacking it without knowing who is behind the incident or his purposes.[380] Needless to say, active self-defense is only possible if the victim is aware that it is under attack. It will not be an option if, as is sometimes the case, the intrusion goes undetected.

Active self-defense fits into the law enforcement framework fairly comfortably. Although hackbacks are probably illegal under the Computer Fraud and Abuse Act[381]—the victims are, after all, perpetrating cyber-intrusions of their own—fundamental principles of criminal law can explain why they might be acceptable if we were writing on a blank slate. The basic idea is justification. Conduct that ordinarily is condemned can become permissible, or even desirable, in certain circumstances.[382] Homicide is typically illegal, but we are allowed to use deadly force against those who pose a threat to our lives or the lives of others. The same might be said of hackbacks. Society ordinarily condemns those who break into others' computers, but one might be justified in hacking a machine to frustrate its attack on one's own system.[383]

Active self-defense is controversial, but it offers one potential benefit that has been largely overlooked in the literature. Like the other regulatory solutions discussed in this Article, hackbacks can incentivize firms to improve the security of their systems. Cyber-perpetrators typically do not launch attacks directly; to obscure their responsibility, they usually route an attack through a chain of unsecured intermediary systems before reaching the ultimate target.[384] If a victim responds to an intrusion with active self-

---

[379] O'Neill, *supra* note 19, at 240, 280; Sklerov, *supra* note 19, at 25 & n.160; *cf.* Richard A. Epstein, *The Theory and Practice of Self-Help*, 1 J.L. ECON. & POL'Y 1, 30 (2005) (emphasizing the need for "self-help remedies").

[380] Condron, *supra* note 19, at 415–16; Jensen, *Computer Attacks*, *supra* note 19, at 232. *See generally supra* notes 116–20 and accompanying text (discussing attribution difficulties).

[381] *See* AM. BAR ASS'N, *supra* note 18, at 18; BAKER, *supra* note 24, at 212; CLARKE & KNAKE, *supra* note 1, at 214; Smith, *supra* note 17, at 180, 182.

[382] *See generally* Joshua Dressler, *Foreword*: *Justifications and Excuses: A Brief Review of the Concepts and the Literature*, 33 WAYNE L. REV. 1155 (1987) (exploring the defense of justification in criminal law).

[383] *See* Katyal, *Community*, *supra* note 135, at 61; O'Neill, *supra* note 19, at 280; Smith, *supra* note 17, at 190–91. *But see* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 448 (2007) (condemning active self-defense as "vigilantism"); Orin S. Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*, 1 J.L. ECON. & POL'Y 197, 204–05 (2005) (same). Hackbacks also can be described in armed conflict terms. Ari and Jeremy Rabkin argue that private citizens who conduct cyber-intrusions with a state's blessing are the equivalent of privateers who operate under state-issued letters of marque. Rabkin & Rabkin, *supra* note 70, at 12–13.

[384] *See supra* note 120 and accompanying text.

defense, it is likely that these third-party systems will be harmed.[385] The realspace analog is a driver who leaves his car unlocked with the keys in the ignition; the car is then stolen by bank robbers and destroyed when the thieves open fire and the bank's security guards shoot back. Many scholars regard this third-party problem as a sufficient reason to forbid hackbacks.[386] Yet the prospect of damage to third parties may have beneficial effects. The threat of harm would incentivize third parties to prevent their systems from being used as conduits for attacks on others. Suppose Citibank knows that, if attackers gain control of its computers and use them to conduct DDOS attacks, the victims will be allowed to retaliate against Citibank's machines. Citibank will have a fairly strong incentive to ensure that its computers are not commandeered into botnets. Damage from hackbacks thus would internalize some of the costs that third parties impose on others by maintaining insecure systems.[387] (Likewise in realspace. If drivers know that security guards are allowed to damage getaway cars even if they are stolen, they will lock their doors.) Active self-defense also might weaken attackers' incentives to commit cyber-attacks. If assailants know that victims will be able to use hackbacks to render their attacks ineffective, or less effective, they will have less reason to undertake them in the first place. By increasing the futility of intrusions, hackbacks can help achieve deterrence.[388] Active self-defense thus can simultaneously foster favorable incentives to improve security and weaken unfavorable incentives to commit attacks.

At the same time, active self-defense has a number of glaring downsides. It seems inequitable to force third parties whose systems have been compromised to bear the costs of the ensuing hackbacks—especially if they are individual users rather than sophisticated firms capable of devoting meaningful sums to cyber-defense.[389] Moreover, as Orin Kerr points out, active self-defense "would create an obvious incentive for attackers to be extra careful to disguise their location or use someone else's computer to launch the attack."[390] Permitting hackbacks also would

---

[385] *See* Epstein, *supra* note 379, at 31; Katyal, *Community*, *supra* note 135, at 62–63; Kerr, *supra* note 383, at 205; Smith, *supra* note 17, at 180.

[386] Katyal, *Community*, *supra* note 135, at 60–66; Kerr, *supra* note 383, at 205–06.

[387] *Cf.* Picker, *supra* note 44, at 116, 136 (discussing externalities that arise from poorly secured computers being used as zombies for DDOS attacks).

[388] *See* O'Neill, *supra* note 19, at 280; Sklerov, *supra* note 19, at 10. *See generally supra* note 261 and accompanying text (explaining how lowering the benefits of cyber-attacks can contribute to deterrence).

[389] These injuries might be partially cured by granting third parties a right against the initial intruder to compensation for all resulting harms, including those caused by a hackback. Of course, this sort of compensation mechanism depends on the ability to identify the initial intruder, and that is often an impossible task. *See supra* notes 116–20 and accompanying text. The possibility of compensation would also weaken third parties' incentives to secure their systems.

[390] Kerr, *supra* note 383, at 205.

"encourage foul play designed to harness the new privileges"; one example is the "bankshot attack," in which an assailant who wants a computer to be attacked "can route attacks through that one computer towards a series of victims, and then wait for the victims to attack back at that computer."[391] It cannot be predicted a priori whether the harmful conduct produced by these negative incentives would be greater or lesser than the beneficial conduct produced by the positive incentives. A good deal more study is needed before an active self-defense regime could be put into place.

CONCLUSION

Cyber-threats aren't going away. As society increasingly comes to rely on networked critical infrastructure such as banks and the power grid, adversaries will find that they have ever more to gain by attacking these digital assets. And we will find that we have ever more to lose.

It therefore becomes essential to think about cyber-security using an analytical framework that is rich enough to account for the problem in all its complexity. Cyber-security is too important, and too intricate, to leave to the criminal law and the law of armed conflict. Instead, as this Article has proposed, an entirely new conceptual approach is needed—an approach that can account for the systematic tendency of many private firms to underinvest in cyber-defense. Companies sometimes fail to secure their systems against attackers because they do not bear the full costs of the resulting intrusions; the harms are partially externalized onto third parties. Firms also tend to neglect cyber-security because by improving their own defenses they contribute to the security of others' systems; the benefits are partially externalized, which creates opportunities for free riding. If these problems sound familiar, that's because they are. These challenges of negative externalities, positive externalities, and free riding are similar to challenges that the modern administrative state encounters in a number of other settings, such as environmental law, antitrust law, products liability law, and public health law. Scholars and lawmakers might look to these other fields for suggestions on how to incentivize private firms to improve their defenses; conceiving of cyber-security in regulatory terms opens the door to regulatory solutions.

Of course, "regulatory solutions" need not mean "command-and-control solutions." Often it will be possible to promote better cyber-security by appealing to firms' self-interest—encouraging them to improve their defenses by immunizing them from liability or offering other subsidies—instead of sanctioning them when they fail to do so. For instance, rather than empowering a central regulator to monitor the Internet for outbreaks of malicious code, companies should use something like public health law's distributed biosurveillance network to collect and share information

[391] *Id.*; *accord* Katyal, *Community*, *supra* note 135, at 62–63.

about cyber-threats. Similarly, the private sector should play an active role in establishing industry-wide cyber-security standards, as it frequently does in environmental law and other regulatory contexts. Offers of immunity and threats of liability then would be used to encourage companies to adopt the agreed-upon standards. And as for improving the ability of critical systems to survive intrusions, infected computers could be temporarily disconnected from the Internet to keep them from spreading the malware, and companies should be encouraged to build their systems with excess capacity (such as reserve bandwidth and remote backups) that can be called into service during cyber-attacks.

Virtually no one is happy with the state of America's cyber-defenses, and scholars have felled entire forests exploring how to prosecute cyber-criminals more effectively or retaliate against countries that launch cyber-attacks. Maybe we've been asking the wrong questions. Maybe what we need to secure cyberspace isn't cops, spies, or soldiers. Maybe what we need is administrative law.