UNIVERSITY *of* PENNSYLVANIA LAW REVIEW

Founded 1852

Formerly
AMERICAN LAW REGISTER

VOL. 162 APRIL 2014 NO. 5

ARTICLE

GHOST IN THE NETWORK

DEREK E. BAMBAUER†

† Professor of Law, James E. Rogers College of Law, University of Arizona. I owe thanks for helpful suggestions and discussion to Kendra Albert, David Ardia, Miriam Baer, Jane Yakowitz Bambauer, Chris Beauchamp, Emily Berman, Bob Brauneis, Annemarie Bridy, Mike Carroll, Susan Crawford, Leslie Francis, Rebecca Green, James Grimmelmann, Woody Hartzog, Rob Heverly, Dan Hunter, Margo Kaplan, Greg Lastowka, Brian Lee, David Levine, Sarah Light, Gregg Macey, Mike Madison, Irina Manta, Toni Massaro, Andrea Matwyshyn, Minor Myers, Thinh Nguyen, Mark Noferi, David Opderbeck, Jim Park, David Post, Nathan Sales, Chris Soghoian, Endre Stavang, Alan Trammell, Tara Urs, Kevin Werbach, Tal Zarsky, Adam Zimmermann, and Jonathan Zittrain; the participants in the Second Annual Internet Law Work-in-Progress Series at New York Law School; the participants in the Cyberlaw Colloquium at Harvard Law School; and the participants in the Rocky Mountain Junior Scholars Conference. I owe thanks for expert research to Maureen Garmon. I welcome comments at derekbambauer@email.arizona.edu.

Cyberattacks are inevitable and widespread. Existing scholarship on cyber-espionage and cyberwar is undermined by its futile obsession with preventing attacks. This Article draws on research in normal accident theory and complex system design to argue that successful attacks are unavoidable. Cybersecurity must focus on mitigating breaches rather than preventing them. First, this Article analyzes cybersecurity's market failures and information asymmetries. It argues that these economic and structural factors necessitate greater regulation, particularly given the abject failures of alternative approaches. Second, this Article divides cyberthreats into two categories: known and unknown. To reduce the impact of known threats with identified fixes, the federal government should combine funding and legal mandates to push firms to redesign their computer systems. Redesign should follow two principles: disaggregation—dispersing data across many locations—and heterogeneity—running those disaggregated components on variegated software and hardware. For unknown threats—"zero-day attacks"—regulation should seek to increase the government's access to markets for these exploits. Regulation cannot exorcise the ghost in the network, but it can contain the damage it causes.

> *Maelcum produced a white lump of foam slightly smaller than Case's head, fished a pearl-handled switchblade on a green nylon lanyard out of the hip pocket of his tattered shorts, and carefully slit the plastic. He extracted a rectangular object and passed it to Case. "Thas part some gun, mon?"*
>
> *"No," said Case, turning it over, "but it's a weapon. It's virus."*
>
> William Gibson
> *Neuromancer* (1984)

INTRODUCTION

Begin with a tale of two specters.

The first invaded the computer systems of the Dalai Lama in Dharamsala, India, sometime in 2008.[1] As the leader of Tibet's government in exile, the Dalai Lama has long attracted the interest and suspicion of the People's Republic of China.[2] The Dalai Lama and the government in exile depend heavily on Internet communications technologies—a dependence exploited by their adversaries.[3]

---

1 INFO. WARFARE MONITOR, TRACKING *GHOSTNET*: INVESTIGATING A *CYBER ESPIONAGE* NETWORK 14 (2009).

2 *Profile: The Dalai Lama*, BBC NEWS (Mar. 10, 2011), http://www.bbc.co.uk/news/world-asia-pacific-12700331.

3 SHISHIR NAGARAJA & ROSS ANDERSON, THE SNOOPING DRAGON: SOCIAL-MALWARE SURVEILLANCE OF THE TIBETAN MOVEMENT 4 (2009), *available at* http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf.

The initial hint of trouble came from diplomacy. The Dalai Lama's staff contacted a diplomatic official by email to arrange a meeting.[4] Before they could arrange a telephone conversation, the diplomat received a warning from the Chinese government not to undertake the meeting.[5] Fearing that its systems had been compromised, the government in exile turned to the OpenNet Initiative (ONI), an academic research consortium that studies Internet censorship.[6] ONI dispatched two affiliated security researchers to analyze the Dalai Lama's computer systems.[7]

What they found was GhostNet: a sophisticated software program capable of covertly capturing keystrokes, copying files, and even activating cameras and microphones attached to infected computers.[8] GhostNet was a near-perfect spy: powerful, flexible, and almost invisible. It had infected computers used by the Dalai Lama, the government in exile, diplomatic offices in the United States and Europe, and a Tibetan activist organization.[9] ONI researchers watched GhostNet steal secret information from computers in the Dalai Lama's personal office, including a document outlining negotiating positions in discussions with the Chinese government.[10] They determined through their investigation that computers located in three different Chinese provinces (and one server rented from a U.S. Internet service provider (ISP)) controlled GhostNet.[11]

The specter was widespread: researchers found that GhostNet had infected nearly 1300 computers in more than 100 countries, including computers in the foreign affairs ministries of Iran and Indonesia; embassies of India, South Korea, and Taiwan; intergovernmental organizations; news organizations; and Tibetan exile groups.[12] Determining attribution—learning who operated GhostNet—was not possible from the data ONI could obtain.[13] The likely answer, though, is that China's security services introduced the ghost into the network.[14]

---

4 *Id.* at 5.

5 *Id.*

6 *Id.* Disclosure: The author worked for the OpenNet Initiative as a research fellow from 2004–2006.

7 *Id.*

8 INFO. WARFARE MONITOR, *supra* note 1, at 5-6.

9 *Id.* at 5; NAGARAJA & ANDERSON, *supra* note 3, at 5-7.

10 INFO. WARFARE MONITOR, *supra* note 1, at 25 & 26 fig.5.

11 *Id.* at 24-25, 30; John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES, Mar. 29, 2009, at A1.

12 INFO. WARFARE MONITOR, *supra* note 1, at 5, 22.

13 *Id.* at 48. *But see* NAGARAJA & ANDERSON, *supra* note 3, at 11 (describing "how agents of the Chinese government compromised the computing infrastructure of the Office of His Holiness the Dalai Lama").

14 *See* INFO. WARFARE MONITOR, *supra* note 1, at 48.

The second specter infiltrated the computers controlling Iran's nuclear enrichment program, likely in 2007.[15] Stuxnet, a joint project of the United States and Israel, is the most advanced cyberweapon built to date.[16] It performed two clever tasks: it sped up the centrifuges that enrich uranium, damaging some irreparably, and it concealed the acceleration from the engineers monitoring the system.[17] Stuxnet recorded data from normal centrifuge operations and, while sabotaging the centrifuges, replayed the normal data to the engineers, falsely reassuring them.[18] One piece of sophisticated malware succeeded where diplomacy and threats of military force failed—it set back Iran's attempts to craft a nuclear weapon by at least a year, and likely longer.[19]

Stuxnet both spied on and changed data, and did so invisibly for years.[20] Iran could not determine the cause of the centrifuge failures.[21] The country's nuclear engineers tried helplessly to solve the problem, even shutting down whole complexes of centrifuges at the first sign of trouble.[22] Stuxnet not only damaged Iran's physical infrastructure, it sapped the confidence of its nuclear experts. It crossed the "air gap" that separated Iran's nuclear computer network from the public Internet, breaching a precaution widely viewed as impenetrable.[23] Stuxnet is the first computer-based attack to cause physical damage; its deployment marks the opening salvo of a new era of cyberwar.[24]

GhostNet was a thief; it stole information from Tibet's exiled government to benefit its masters—probably China's government. Stuxnet was a vandal; it fed false data to Iranian nuclear engineers while it slowly destroyed their equipment. In combination, these ghosts demonstrate cybersecurity's most

---

15 David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1.

16 Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1.

17 William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; Christopher Williams, *Stuxnet: Cyber Attack on Iran 'Was Carried Out by Western Powers and Israel,'* TELEGRAPH (London) (Jan. 22, 2011), http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html.

18 Sanger, *supra* note 15.

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

23 Zetter, *supra* note 16; *see also, e.g.*, Eric Knapp, *Bridging the Air Gap: Examining Attack Vectors into Industrial Control Systems*, SECURITYWEEK (Aug. 4, 2011), http://www.securityweek.com/bridging-air-gap-examining-attack-vectors-industrial-control-systems ("[T]he ideal of the air gap is valid and . . . true separation is a viable goal.").

24 Sanger, *supra* note 15.

profound legal and technical challenge—to craft a system that keeps uninvited users from accessing or altering data. This Article proposes an approach to address that challenge. Cybersecurity cannot prevent the ghost in the network; instead, it should seek to cabin its depredations. Mitigation—not prevention—is the key. This Article employs the insights from studies of complex system design, such as normal accident theory, to propose a mixture of legal and technical strategies to deal with both known vulnerabilities and unknown, "zero-day attack[s]."[25]

This proposal builds on my prior work that established a theoretical, information-based approach to cybersecurity.[26] In brief, this methodology approaches cybersecurity as comprising three issues: access, alteration, and integrity of data.[27] Access involves whether a user may reach a given datum.[28] Alteration describes whether she may change it.[29] Integrity asks whether one may determine whether a given piece of information reflects the latest authorized changes.[30] Access and alteration have both positive and negative aspects.[31] The positive range, which I explored in earlier work, considers how authorized users may obtain and update information.[32] This Article explores the negative range of access and alteration: How can regulation reduce attackers' ability to access and alter information stored in networked computer systems?

It leads a new wave of scholarship on cybersecurity that breaks free from extant, poorly fitting models such as criminal law, international law, and the law of armed conflict.[33] This second wave of research develops new models for the unique challenges of information security in a computer environment

---

25 *See* Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World* 1 (Oct. 18, 2012) (paper presented at the 19th ACM Conference on Comp. & Commc'ns Sec.), *available at* http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf ("A *zero-day attack* is a cyber attack exploiting a vulnerability that has not been disclosed publicly. There is almost no defense against a zero-day attack . . . .").

26 *See generally* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584 (2011).

27 *Id.* at 587.

28 *Id.* at 628.

29 *Id.* at 630.

30 *Id.* at 632-33.

31 *Id.* at 628, 630.

32 *Id.*

33 *See id.* at 588-90 (explaining the distinct nature of cybersecurity and scholars' unsuccessful attempts to fit it into preexisting frameworks—especially those involving intent); Michael J. Glennon, *State-Level Cybersecurity*, POL'Y REV., Feb.–Mar. 2012, at 85, 86-87 (explaining that issues of cybersecurity do not fit into existing categories); *see also* Hans Brechbühl et al., *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*, 16 INFO. TECH. FOR DEV. 83, 85 (2010) ("Responding to current and past incidents and attacks requires knowledge of what has happened, methods of preventing similar incidents from being successful in the future, and possible legal or other remedial actions against the perpetrators.").

of ubiquitous connectivity and minimal attribution.[34] Scholars have explored ways that the President, states, and administrative agencies can combat cyberattacks, using models ranging from public health to environmental law.[35] Most important, there is a nascent realization that since it is impossible to completely solve cybersecurity problems, "[w]e must learn to live with the disease."[36] However, this insightful literature identifies a variety of new approaches without offering concrete proposals to augment cybersecurity. This Article fills that gap.

I use an information-based methodology to make a counterintuitive set of arguments about how law can concretely address cybersecurity. My approach begins with the core normative claim that cybersecurity is underregulated. For the past fifteen years, the principal methods of addressing cybersecurity problems have concentrated on voluntary measures through self-regulation[37] and on process-based methodologies to tailor precautions to each organization's requirements.[38] These approaches disdain regulatory mandates. Not coincidentally, all have failed to improve security. Legal

---

[34] *See, e.g.*, 15 U.S.C. § 7262 (2012) (requiring most publicly traded companies to certify the effectiveness of internal controls for financial reporting, implementing section 404 of the Sarbanes–Oxley Act); Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 (2006) (creating a framework for cybersecurity on federal networks and recognizing the unique challenges created by these networks); *see also* Lawrence A. Gordon et al., *The Impact of the Sarbanes–Oxley Act on the Corporate Disclosures of Information Security Activities*, 25 J. ACCT. & PUB. POL'Y 503, 528-29 (2006) (reviewing empirical evidence suggesting the Sarbanes–Oxley Act is leading to greater focus on corporate information security activities).

[35] *See* L. Jean Camp, *Reconceptualizing the Role of Security User*, DAEDALUS, Fall 2011, at 93, 100-02 (engaging end users in creating a secure online environment); Glennon, *supra* note 33, at 100-02 (arguing that states should play a prominent role in securing computing infrastructure); Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, DAEDALUS, Fall 2011, at 70, 75-78 (conceptualizing cybersecurity as a public health challenge); David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 812-29 (2012) (assessing the scope of the President's constitutional authority to combat cyberattacks); Nathan A. Sales, *Regulating Cybersecurity*, 107 NW. U. L. REV. 1503, 1550-51 (2013) (using administrative law concepts to analyze how regulation can address underlying externality problems in cybersecurity); David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. (forthcoming 2014) (manuscript at 61-70), *available at* http://papers.ssrn.com/id=2241838 (evaluating the relative merits of top-down regulation, administrative rulemaking, and delegation to regulated entities in improving cybersecurity through empirical analysis of security breaches).

[36] Simson L. Garfinkel, *The Cybersecurity Risk*, COMM. ACM, June 2012, at 29, 32.

[37] *See generally, e.g.*, N. AM. ELEC. RELIABILITY CORP., CYBER SECURITY—ELECTRONIC SECURITY PERIMETER(S) (2012), *available at* http://www.nerc.com/files/CIP-005-5.pdf (describing the steps taken by a private entity to protect itself from cybersecurity threats).

[38] *See, e.g.*, 15 U.S.C. § 7262 (2012) (providing guidelines for "management assessment of internal controls"); *AWS ISO 27001 FAQs*, AMAZON WEB SERVICES, http://aws.amazon.com/compliance/iso-27001-faqs (last visited Mar. 22, 2014) (describing Amazon Web Services' compliance with an international standard for private entities to protect themselves from cybersecurity threats).

regulation has far more potential to remedy cybersecurity weaknesses than scholars or legislators appreciate. Legal mandates are likely to be costly in places, and to generate substantial political opposition, but they are both possible and desirable.

Next, this Article argues that there are two core problems related to unauthorized access to and alteration of data: attacks with available countermeasures and zero-day attacks without extant defenses (or at least defenses unavailable to anyone other than the attacker).[39] These two categories can be more easily understood as the "known unknowns" and the "unknown unknowns."[40] The key to combating both sets of unknowns is to concentrate on mitigation rather than prevention. Effective mitigation can helpfully reduce attacks in the first place: hackers are less likely to test defenses when success will not bear fruit.[41]

For the *known* unknowns, such as the Structured Query Language (SQL) injection attack against Yahoo!, two mitigation measures are vital: (1) dispersing information widely and in partial form, and (2) storing it under varying conditions.[42] This Article refers to these goals as disaggregation and heterogeneity, or, more colloquially, "divide and differ." This practice reduces the effects of inevitable intrusions and protects against catastrophic failure. To effectuate the "divide and differ" approach, regulation should come in two parts: the carrot and the stick. First, firms that transact business with the government should be required to undertake meaningful steps to achieve disaggregation and heterogeneity. Second, Congress should require that a core set of industries implement measures to divide and differentiate their data stores, with the palliative of federal funding to assist their efforts.

The United States should attempt to convert the *unknown* unknowns, such as the Stuxnet attack on Iran, to *known* unknowns.[43] The best, and perhaps only, strategy concentrates on the growing trade in zero-day attacks

---

39 *See generally* Bambauer, *Conundrum*, *supra* note 26, at 628-32.

40 These terms are borrowed from former Secretary of Defense Donald Rumsfeld, who said, "[T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know." U.S. Dep't of Def., DOD News Briefing—Secretary Rumsfeld and Gen. Myers (Feb. 12, 2002), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636.

41 *See, e.g.*, Huseyin Cavusoglu, *Economics of IT Security Management* ("Security investments . . . act as a deterrent for attackers by making attacks less attractive."), *in* ECONOMICS OF INFORMATION SECURITY 71, 79 (L. Jean Camp & Stephen Lewis eds., 2004).

42 *See, e.g.*, Gery Menegaz, *SQL Injection Attack: What Is It, and How to Prevent It*, ZDNET (July 13, 2012), http://www.zdnet.com/sql-injection-attack-what-is-it-and-how-to-prevent-it-7000000881.

43 *Cf.* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1061-62 (2011) (noting a sharp increase in the incidence of zero-day vulnerabilities).

on the private market. Congress should adopt two statutory rules: mandatory participation in such markets by the federal government and required confidential reporting by firms who trade in these cyberweapons. In addition, Congress should fund a reward program—a "bug bounty"—for researchers who discover zero-day vulnerabilities and agree to sell this information exclusively to the U.S. government.[44]

This Article proceeds in four parts. Part I explains why focusing efforts principally on preventing cyberattacks is misguided: perfect security is impossible, and even attaining good security is extraordinarily difficult. Instead, cybersecurity regulation should concentrate on mitigating the damage that successful attacks cause. Part II sets out the case for regulatory intervention. It explains the core problem of security externalities, demonstrates the failure of alternative approaches, and builds the case for a greater role for law in cybersecurity. Part III elucidates how to address the known unknowns via disaggregation and heterogeneity. Part IV evaluates how best to mitigate the challenges of zero-day attacks that use unknown vulnerabilities and have no known defenses, arguing that the federal government should seek to acquire information in this area. This Article concludes by assessing the challenges of regulating cybersecurity and sketching the next phase of research.

I. KING CANUTE'S CYBERSECURITY

Perfect cybersecurity is folly. Pursuing it risks forgetting the lesson of King Canute, who commanded the tides to halt and, when they ignored him, pointed out his order's futility.[45] Scholars and analysts bemoan the ubiquity of cybersecurity problems such as malware, software flaws, and data breaches.[46] Like the poor, though, these problems will ever be with us.[47] This Part makes three points. First, the complexity of information

---

44 *Cf.* Thomas Claburn, *Google Ups Bug Bounties Amid Booming Exploit Market*, INFORMATIONWEEK (Aug. 16, 2012), http://www.informationweek.com/security/management/google-ups-bug-bounties-amid-booming-exp/240005721 (noting that Google has increased its payments to people who report vulnerabilities in their products); *About,* ZERO DAY INITIATIVE, http://www.zerodayinitiative.com/about (describing a program designed to promote software-vulnerability reporting via monetary incentives).

45 *E.g.*, Kathryn Westcott, *Is King Canute Misunderstood?*, BBC NEWS MAG. (May 26, 2011), http://www.bbc.co.uk/news/magazine-13524677.

46 *See, e.g.*, Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 438 (2012) ("Cyber intrusions can be devastating and can come from sources ranging from unsophisticated teenagers, to high-tech cyber criminals, to military officials."); *How the Experts Would Fix Cyber Security*, BLOOMBERG BUSINESSWEEK (Aug. 2, 2012), http://www.businessweek.com/articles/2012-08-02/how-the-experts-would-fix-cyber-security ("Cyber crime is increasing in frequency and severity.").

47 *See Matthew* 26:11 (King James) ("For ye have the poor always with you . . . .").

technology and the limited testing cycle available to vendors mean vulnerabilities are inevitable. Second, exposure to the Internet means that attackers will locate and exploit those flaws. Thus, failure is inevitable. Finally, and most important, complex system design studies—in particular, research on normal accident theory—show that the right approach to such inevitable failure is to limit the damage caused. Mitigation is a topic almost entirely ignored by legal scholars and legislators, yet vital to meeting cybersecurity threats.

A. *It's Complicated*

Modern software and hardware are simply too complex for flaws to be eliminated completely. The sheer size of programs confounds efforts to detect and remove bugs, and the size is ever-increasing. Microsoft Windows NT 3.1 (the more secure version of Microsoft's two Windows operating systems in 1993) had four to five million lines of code; Windows XP, released eight years later, had thirty-five to forty million.[48] Windows Vista likely had fifty million.[49] As the size of the code base and the number of developers who work on it grow, coordination costs increase.[50] It becomes more difficult for programmers to ensure that different parts of the software interoperate effectively and securely.[51] Even as a theoretical matter, it is difficult to demonstrate that software above a small size (in terms of lines of code) can be completely secure.[52] As a practical matter, it is impossible.

In addition, the complicated interactions among applications, operating systems, and hardware present opportunities for attacks.[53] The Windows ecosystem includes applications, drivers, and firmware—all of which change on an irregular schedule and must remain "compatibl[e] with legacy hardware and

---

48 *E.g.*, Larry O'Brien, *How Many Lines of Code in Windows?*, KNOWING.NET (Dec. 6, 2005), http://www.knowing.net/index.php/2005/12/06/how-many-lines-of-code-in-windows; *see also* Steve Lohr & John Markoff, *Windows Is So Slow, but Why?*, N.Y. TIMES, Mar. 27, 2006, at C1 (stating that Microsoft is slow to develop new versions of Windows because of its large and onerous code base).

49 Lohr & Markoff, *supra* note 48.

50 *See, e.g.*, Caryn A. Conley & Lee Sproull, *Easier Said than Done: An Empirical Investigation of Software Design and Quality in Open Source Software Development* 2 (Jan. 7, 2009) (paper presented at the 42nd Haw. Int'l Conference on Sys. Scis.), *available at* http://www.computer.org/csdl/proceedings/hicss/2009/3450/00/09-14-05.pdf ("As the number of components increases in more modular software, functionality becomes more specialized and isolated . . . and each component contains less functionality on average." (citations omitted)).

51 *See, e.g.*, Claire Le Goues et al., *The Case for Software Evolution* 206 (Nov. 7, 2010) (paper presented at the 18th FSE/SDP Workshop on the Future of Software Eng'g Res.), *available at* http://www.cs.cmu.edu/~clegoues/docs/legoues-foser10.pdf (explaining that software can be thought of as a complex, evolving system, similar to a biological organism).

52 *E.g.*, Mulligan & Schneider, *supra* note 35, at 72-73.

53 *E.g.*, Le Goues et al., *supra* note 51, at 207.

software."[54] Standard programming responses to this problem, such as modularity (ensuring that components are independent of one another such that failures are not concatenated), have mixed results at best. An empirical study of Java-based programs available from the popular open-source repository SourceForge found, counterintuitively, that greater software modularity is associated with an increase in the number of bugs.[55] This contradicts the conventional wisdom that modularity enhances software quality.[56] Similarly, despite a wealth of methods including improved testing suites, coding best practices, enhanced specifications, and specific techniques for combating errors such as buffer overflows, "software today remains, in many ways, far less reliable and more prone to bugs than in the past."[57]

Software is thus structurally prone to failure, despite significant efforts to remediate it. Maintenance, including bug fixes, can consume "up to 90% of the cost of a typical software project, at a total cost of up to $70 billion per year in the [United States]."[58] These costs result not only from software complexity, but also from the challenges of organizational change (and concomitant changes in demands on software) and from poor software design.[59] Further, it is far more costly to fix bugs late in the development cycle.[60] Yet even companies such as Microsoft, which take software security design seriously, suffer from bugs and attacks.[61] The firm delayed the release of Windows Vista to improve security, yet the operating system still shipped with vulnerabilities that were rapidly exploited by hackers.[62] Eliminating bugs completely is simply impossible.

---

54 Lohr & Markoff, *supra* note 48.

55 *See, e.g.*, Conley & Sproull, *supra* note 50, at 9-10.

56 *Id.*

57 Le Goues et al., *supra* note 51, at 205.

58 *Id.* (footnotes omitted).

59 *See, e.g.*, Kenneth C. Laudon & Jane P. Laudon, *Securing Information Systems*, *in* ESSENTIALS OF MANAGEMENT INFORMATION SECURITY 1, 2 (8th ed. 2008).

60 *Id.*

61 *E.g.*, John Markoff, *Stung by Security Flaws, Microsoft Makes Software Safety a Top Goal*, N.Y. TIMES, Jan. 17, 2002, at C1.

62 *See, e.g.*, Philip Bethge, *Microsoft Development Head: 'The Whole Room Will Be the Computer,'* SPIEGEL ONLINE INT'L (Oct. 24, 2012), http://www.spiegel.de/international/world/microsoft-development-leader-craig-mundie-on-the-future-of-computers-a-863103.html (interviewing Microsoft's development director Craig Mundie); Ryan Naraine, *Remote Exploit Released for Windows Vista SMB2 Worm Hole*, ZDNET (Sept. 17, 2009), http://www.zdnet.com/blog/security/remote-exploit-released-for-windows-vista-smb2-worm-hole/4350 (discussing a "team of exploit writers" who attacked a vulnerability in Windows Vista); Ryan Naraine, *Vista Exploit Surfaces on Russian Hacker Site*, EWEEK (Dec. 22, 2006), http://www.eweek.com/c/a/Security/Vista-Exploit-Surfaces-on-Russian-Hacker-Site (stating that Microsoft was monitoring and fixing a vulnerability in Windows Vista that was identified on a Russian website).

B. *Exposure*

The Internet makes securing code much harder by exposing the inevitable bugs in software to sustained scrutiny and attack. Many—if not most—computers are connected to the Internet directly or indirectly. This provides a path for attack and enables hackers to test and then compromise systems that were never designed for public networks. Such systems include utility companies' Supervisory Control and Data Acquisition (SCADA) controllers, many of which employ hard-coded passwords.[63] GarrettCom, which claims to provide equipment to seventy-five percent of the top one hundred power companies in North America, built a hidden account with a hard-coded password into a switch management application accessible online.[64] RuggedCom's Rugged Operating System had both a "hard-coded RSA SSL private key" and a "factory account" that could be exploited by attackers.[65] Administrative conveniences transform into critical weaknesses when connected to the Internet, which exposes devices and programs designed for networks protected by physical safeguards to worldwide scrutiny.

Moreover, attackers—those who seek to locate and exploit vulnerabilities in software—have considerable informational advantages over defenders. Attackers have more time; software vendors are profit-driven and must release code to the public under the constraints of release cycles and quarterly earnings statements.[66] Once software is publicly available, however, attackers can test it at their leisure.[67] This raises the second advantage:

---

63 *See* Kelly Jackson Higgins, *SCADA Security in a Post-Stuxnet World*, DARK READING (Nov. 6, 2012), http://www.darkreading.com/vulnerability/scada-security-in-a-post-stuxnet-world/240049917.

64 *Advisory (ICSA-12-243-01): GarrettCom—Use of Hard-Coded Password*, ICS-CERT, https://ics-cert.us-cert.gov/advisories/ICSA-12-243-01 (last updated Apr. 30, 2013); *see also* Richard Chirgwin, *Insecure SCADA Kit Has Hidden Factory Account, Password*, REGISTER (Sept. 5, 2012), http://www.theregister.co.uk/2012/09/05/more_insecure_scada (describing the ICS-CERT advisory and its impact).

65 Lucian Constantin, *ICS-CERT Warns of SSL Security Flaw in RuggedCom Industrial Networking Devices*, COMPUTERWORLD (Aug. 22, 2012), http://www.computerworld.com/s/article/9230516/ICS_CERT_warns_of_SSL_security_flaw_in_RuggedCom_industrial_networking_devices (internal quotation marks omitted).

66 *See* William Yurcik & David Doss, *CyberInsurance: A Market Solution to the Internet Security Market Failure* (May 17, 2002) (paper presented at the 2d Workshop on Econ. and Info. Sec.), *available at* http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/53.pdf (explaining that market pressures practically guarantee the existence of exploitable software flaws); *cf.* Mike Sutton & Tym Moore, *7 Ways to Improve Your Software Release Management*, CIO (July 30, 2008), http://www.cio.com/article/440101/7_Ways_to_Improve_Your_Software_Release_Management (noting time constraints and other market pressures affecting the release of companies' software projects).

67 *Cf.* JOHN VIEGA, THE MYTHS OF SECURITY 139-44 (2009) ("There are many, many more vulnerabilities than are publicly disclosed. Some are found and fixed, but there will always be many securities that are never found.").

attackers have greater numbers.[68] Software companies and security research firms have limited staff. Hackers operate worldwide and benefit from widespread distribution of automated cracking tools such as fuzzers, as well as from the results of employing those tools.[69] Third, hackers have a lead-time advantage: once a vulnerability is discovered, it takes the vendor time to understand the problem (assuming they learn about it simultaneously, which is rare) and to patch it.[70] Thus, there is an inevitable window during which systems are insecure.

Lastly, even perfect security against external attacks cannot guard against turncoats and mistakes. Cybersecurity cannot prevent those who are authorized to access information from sharing it with those who are not.[71] One cybersecurity survey found that insiders launched one in every five attacks.[72] For instance, even if Private Bradley Manning had not been able to download data from the Department of Defense's SIPRNet intelligence network, Manning could have revealed memorized information to others.[73] Systems disconnected from the Internet are still vulnerable to insider attack: Stuxnet compromised an air-gapped system.[74] Someone in Iran's nuclear program either deliberately or inadvertently infected its computer systems with the virus. And even secure software can be misconfigured. Incorrect security settings on shared network drives, for example, left sensitive data for over 350,000 University of North Carolina at Charlotte

---

68 *Cf.* ERIC RAYMOND, THE CATHEDRAL & THE BAZAAR 36-38 (1999) (noting that the greater number of testers for open source software increases bug detection).

69 *See* Scott Lambert, *Fuzz Testing at Microsoft and the Triage Process*, SECURITY DEV. LIFECYCLE BLOG (Sept. 20, 2007), http://blogs.msdn.com/b/sdl/archive/2007/09/20/fuzz-testing-at-microsoft-and-the-triage-process.aspx (demonstrating how information from fuzzers can be widely disseminated).

70 VIEGA, *supra* note 67, at 221-22.

71 *See, e.g.*, Steven R. Chabinsky, *Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*, 4 J. NAT'L SECURITY L. & POL'Y 27, 34-35 (2010) ("Current employees, contractors, and trusted business partners have a unique opportunity to do . . . harm because they have been provided authorized access to . . . physical and digital spaces."); Alan Joch, *Why You Can't Stop Insider Threats*, FCW (Feb. 28, 2011), http://fcw.com/articles/2011/02/28/feat-cybersecurity-insider-threats.aspx ("Some of the most damaging security breaches originate from inside an agency's firewalls.").

72 Joch, *supra* note 71.

73 David Leigh, *How 250,000 US Embassy Cables Were Leaked*, GUARDIAN (Nov. 28, 2010), http://www.guardian.co.uk/world/2010/nov/28/how-us-embassy-cables-leaked. *See generally* Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311 (2011). Private Manning now identifies as Chelsea. Adam Gabbatt, *"I Am Chelsea Manning," Says Jailed Soldier Formerly Known as Bradley*, GUARDIAN (Aug. 22, 2013), http://www.theguardian.com/world/2013/aug/22/bradley-manning-woman-chelsea-gender-reassignment.

74 Sanger, *supra* note 15.

students and employees exposed for nearly *fifteen years*.[75] A survey of attendees of the hacker conference, DEFCON 18, revealed that 73% found misconfigured networks in three out of every four clients with whom they worked.[76] Thus, "88% believe the biggest threat to organizations lies inside the firewall."[77] This sets a limit on how effective cybersecurity can be: the human element cannot be completely eliminated.

The combination of vulnerabilities and Internet exposure means that failures of seemingly invulnerable systems are legion. RSA's SecurID 800 tokens, which are widely used to safeguard authentication credentials, were cracked using an attack against the tokens' encryption algorithm.[78] RSA itself suffered a breach that revealed the "seeds" used with its cryptographic algorithm to generate the numbers employed by the SecurID tokens for authentication.[79] Google, Adobe, and other software firms suffered intellectual property theft in 2010 when attackers—likely based in China—used a zero-day vulnerability in Microsoft Internet Explorer to break into their networks.[80] Telvent, which makes control hardware and software for utilities, had its systems penetrated, probably by hackers based in China.[81] The attackers not only gained access to Telvent's code and left behind malware on its network, but may have had access to Telvent customers' project files and networks.[82] Attackers based in China used a USB drive–based vector to obtain data from India's navy, even though the navy's network was not connected to the Internet.[83] Two weeks after Microsoft triumphantly released a new tool designed to reduce exploitation of security

---

75 Anne Saita, *UNC–Charlotte Data Breaches Expose 350,000 Social Security Numbers and Much More*, THREATPOST (May 11, 2012), http://threatpost.com/unc-charlotte-data-breaches-expose-350000-social-security-numbers-and-much-more-051012/76552.

76 *Misconfigured Networks Main Cause of Breaches*, HELP NET SECURITY (Aug. 31, 2010), http://www.net-security.org/secworld.php?id=9801.

77 *Id.*

78 Dan Goodin, *Scientists Crack RSA SecurID 800 Tokens, Steal Cryptographic Keys*, ARS TECHNICA (June 25, 2012), http://arstechnica.com/security/2012/06/securid-crypto-attack-steals-keys.

79 Peter Bright, *RSA Finally Comes Clean: SecurID Is Compromised*, ARS TECHNICA (June 6, 2011), http://arstechnica.com/security/2011/06/rsa-finally-comes-clean-securid-is-compromised.

80 Dan Goodin, *IE Zero-Day Used in Chinese Cyber Assault on 34 Firms*, REGISTER (Jan. 14, 2010), http://www.theregister.co.uk/2010/01/14/cyber_assault_followup.

81 Kim Zetter, *Maker of Smart-Grid Control Software Hacked*, WIRED (Sept. 26, 2012), http://www.wired.com/threatlevel/2012/09/scada-vendor-telvent-hacked.

82 Brian Krebs, *Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent*, KREBS ON SECURITY (Sept. 26, 2012), http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent.

83 Sean Gallagher, *Chinese Hackers Steal Indian Navy Secrets with Thumbdrive Virus*, ARS TECHNICA (July 2, 2012), http://arstechnica.com/security/2012/07/chinese-hackers-steal-indian-navy-secrets-with-thumbdrive-virus.

vulnerabilities, an independent researcher demonstrated code that bypassed it.[84] Of the 200,000 most popular websites that use Secure Sockets Layer (SSL)—the encryption protocol users have been trained to look for on e-commerce sites—fewer than 10% had properly implemented patches to remedy known SSL weaknesses.[85] No matter how secure a system seems, the combination of complexity and exposure puts it at risk.

Inevitably, there will be more security failures.

C. *Plan for the Crash*

Prevention, while worthwhile, is imperfect. Security failures are inevitable. This Article draws upon the burgeoning literature that examines why accidents occur, even in expert organizations that stress competence, prevention, and learning. These studies go by different names in different fields—normal accident theory, high reliability theory, and error management—but regardless of the rubric, their findings hold lessons of critical importance for cybersecurity. Most important, complex system design principles suggest that, under conditions of inevitable failure, regulation should seek to limit the effects of that failure, rather than prevent it.[86] This reduces the effects of successful cybersecurity attacks by impeding the attacker's ability to use information once accessed or to alter data without detection. Such efforts also augment prevention: hackers are less likely to launch attacks as their payoff from such attacks declines.

Studies of complex systems in disparate areas—aviation,[87] nuclear power,[88] medicine,[89] and space exploration[90]—demonstrate that failures are inevitable.

---

84 Dan Goodin, *Microsoft Defense That Fetched $50,000 Prize Bypassed in Just 2 Weeks*, ARS TECHNICA (Aug. 8, 2012), http://arstechnica.com/security/2012/08/microsoft-defense-bypassed-in-2-weeks.

85 Dan Goodin, *90% of Popular SSL Sites Vulnerable to Exploits, Researchers Find*, ARS TECHNICA (Apr. 26, 2012), http://arstechnica.com/business/2012/04/90-of-popular-ssl-sites-vulnerable-to-exploits-researchers-find.

86 *See generally* CHARLES PERROW, THE NEXT CATASTROPHE: REDUCING OUR VULNERABILITIES TO NATURAL, INDUSTRIAL, AND TERRORIST DISASTERS (2007).

87 *See generally* Robert L. Helmreich, *Managing Human Error in Aviation*, SCI. AM., May 1997, at 62 ("[W]ell-trained and technically proficient crews could crash airworthy craft because of failures of human interaction and communication . . . .").

88 *See, e.g.*, CHARLES PERROW, NORMAL ACCIDENTS 15-61 (1984) (discussing the Three Mile Island accident and generally discussing nuclear power as a high-risk system).

89 *See, e.g.*, Elise C. Becher & Mark R. Chassin, *Improving Quality, Minimizing Error: Making It Happen*, HEALTH AFF., May/June 2001, at 68, 71 ("[E]ven the most highly trained and proficient [medical] professionals occasionally make mistakes.").

90 *See generally* DIANE VAUGHAN, THE CHALLENGER LAUNCH DECISION: RISKY TECHNOLOGY, CULTURE AND DEVIANCE AT NASA 389 (1996) (noting that "complex structural causes" led to the crash of the *Challenger*).

Efforts to reduce them are worthwhile; but complete prevention is impossible, and "[t]he best that organisations can hope for is to manage error effectively, decreasing the probability of errors and minimising their consequences."[91] This Article, unlike other cybersecurity scholarship, focuses on managing error effectively, rather than on eliminating it. This approach is aligned with approaches taken to address problems in other complex, technical systems.

In particular, social scientists have begun to study critical infrastructure, where a means of managing error effectively would be a welcome innovation.[92] Such infrastructure, unfortunately, tends to be difficult to operate without error: its systems are networked, it is composed of multiple interdependent entities, and it has heterogeneous technical characteristics due to growth over time.[93] Furthermore, it faces increasingly numerous challenges, from hostile actors to resource limitations to the potentially devastating consequences of failure.[94]

For example, nuclear power plants involve complicated technology that carries significant risk: failures such as those at Three Mile Island and Chernobyl are extremely rare, but potentially catastrophic. As sociologist Charles Perrow has documented, the problems are exacerbated by the combination of imperfect information, regulatory capture, and simple bad luck.[95] Indeed, the recent disaster at Japan's Fukushima plant demonstrated all three attributes.[96] But at base, there is an irreducible risk of failure in complex systems that are tightly coupled, where failure in one area creates a cascade. To prevent these "normal accidents," one must redesign the system: architecting the system to loosen its coupling and reduce its complexity.[97] Unfortunately, with the Internet, network effects mean that redesign is improbable at best, and impossible at worst.[98] There will always be accidents.

---

91 Robert L. Helmreich, *Error Management as Organisational Strategy*, *in* PROCEEDINGS OF THE IATA HUMAN FACTORS SEMINAR 1, 1 (1998).

92 "Critical infrastructure" is a vexed and nearly formless term in cybersecurity. One research group defines it pragmatically as "core technical capabilities, along with the organizations that provide them, that enable the provision of a wide variety of social activities, goods, and services." EMERY ROE & PAUL R. SCHULMAN, HIGH RELIABILITY MANAGEMENT 6 (2008).

93 *Id*.

94 Todd R. LaPorte, *Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise*, 15 J. CONTINGENCIES & CRISIS MGMT. 60, 61-62 (2007) (listing the myriad challenges that face first and second responders to catastrophic events).

95 Charles Perrow, *Fukushima and the Inevitability of Accidents*, 67 BULL. ATOMIC SCIENTISTS 44, 50-51 (2011).

96 *Id*. at 45-50.

97 *Id*. at 51.

98 *See* Bambauer, *Conundrum*, *supra* note 26, at 598-601 (discussing barriers to Internet redesign that arise from network effects).

Two competing theories dominate the study of error, particularly in critical infrastructure. The first, normal accident theory, builds on the work of James Reason,[99] Barry Turner,[100] and Charles Perrow.[101] This theory characterizes technical systems along two dimensions: coupling and interactivity.[102] A tightly coupled system is highly efficient, but has little backup capacity, tolerance for delay, or flexibility in the sequence in which tasks must be performed.[103] Loosely coupled systems have greater reserves, the ability to reorder production activities, and slack capabilities.[104] Systems with little interactivity—which Perrow calls "linear systems"—may have many components, but each component has a single function, and the effects from its behavior on other segments are easily predicted.[105] For these systems, even unplanned events are readily visible to operators.[106] Complex systems, by contrast, have components with multiple uses, and these components interact with multiple other components.[107] Such systems tend to result in unexpected events that are less visible and more difficult to understand.[108] Tightly coupled and complex systems inevitably have accidents: unplanned events develop quickly from underlying design risks and evade remediation techniques.[109]

The second complex system design theory, called "high reliability theory," accepts normal accident theory's framework, but not its conclusions.[110] High reliability theory studies tightly coupled and complex systems, where certain catastrophic events cannot be allowed to occur. According to this theory, they do not occur—otherwise, system failure would result.[111] A nuclear power plant cannot permit a reactor-core meltdown, and air-traffic-control systems cannot allow plane crashes. A key goal of high reliability theory is to identify and elucidate the characteristics that enable such

---

99 *See generally* JAMES REASON, HUMAN ERROR (1990).

100 *See generally* BARRY A. TURNER, MAN-MADE DISASTERS (1978).

101 *See generally* PERROW, *supra* note 88.

102 *Id.* at 72.

103 *Id.* at 89-94.

104 *Id.*

105 *Id.* at 72-79.

106 *Id.* at 78-79.

107 *Id.* at 72-79.

108 *Id.* at 78-79.

109 ROE & SCHULMAN, *supra* note 92, at 54.

110 *See, e.g.*, Todd R. La Porte, *High Reliability Organizations: Unlikely, Demanding and at Risk*, 4 J. CONTINGENCIES & CRISIS MGMT. 60, 60-61 (1996) (introducing the approach taken by the High Reliability Organization Project).

111 Todd R. LaPorte & Paula M. Consolini, *Working in Practice but Not in Theory: Theoretical Challenges of "High-Reliability Organizations,"* 1 J. PUB. ADMIN. RES. & THEORY 19, 20 (1991).

organizations and systems to operate without error.[112] These characteristics include the following: defined states that indicate the system is moving toward a catastrophic event, organizational culture that prizes watchfulness and error reporting, and flexible organizational relationships during crises.[113]

These two theories are eternally at war. High reliability theory claims to solve the problem that normal accident theory believes is unsolvable. Normal accident theory views "high reliability organizations" as lucky in time: their catastrophes simply have not happened yet. Yet both theories suffer from internal flaws and ungrounded assumptions.[114]

This Article adopts normal accident theory as its approach for four reasons. First, the high-reliability-theory approach is untenable for cybersecurity. For cybersecurity purposes, "catastrophic" states lack coherent, precise definitions. The definitional ambiguities are linked to the fuzzy, apocalyptic rhetoric about cybersecurity threats.[115] Not all cybersecurity flaws or errors are created equal, and conditions to be avoided are variegated: preventing an attacker from accessing the network, reading data, or shutting down the electrical grid are possible responses to pending attacks of very different magnitudes. This stratification means that organizations cannot develop succinct procedures to avoid a catastrophic state, or indicators that warn of its approach.[116]

Second, few if any organizations involved in cybersecurity can adopt the single-minded focus on preventing crises that holds for nuclear aircraft carriers or for the electrical grid. High reliability organizations are characterized by close regulatory oversight and significant investment in precautions.[117] Unfortunately, there is already massive resistance to cost and regulation on the cybersecurity front, and security is at best a secondary goal for most organizations.[118]

Third, because many cybersecurity errors occur without significant adverse consequences, organizations can engage in iterative learning through

---

112 *See, e.g.*, David P. Baker, Rachel Day & Eduardo Salas, *Teamwork as an Essential Component of High-Reliability Organizations*, 41 HEALTH SERVICES RES. 1576, 1585-90 (2006) (arguing that teamwork is one such characteristic).

113 ROE & SCHULMAN, *supra* note 92, at 54-56 & fig.4.1.

114 *Id.* at 57-58. Roe and Schulman also argue that both theories neglect management's role as a mechanism for preventing and then buffering error. *Id.*

115 *See generally* Bambauer, *Conundrum*, *supra* note 26, at 603-20.

116 JAMES REASON, MANAGING THE RISKS OF ORGANIZATIONAL ACCIDENTS 192-99 (1997).

117 ROE & SCHULMAN, *supra* note 92, at 54.

118 *See, e.g.*, VIEGA, *supra* note 67, at 141-44 (discussing software developers' lackluster commitment to security); Chris Strohm, *Napolitano Counters Industry on Cost of Cybersecurity Bill*, BLOOMBERG (Feb. 16, 2012), http://www.bloomberg.com/news/2012-02-16/napolitano-counters-industry-on-cost-of-cybersecurity-measure.html.

experimentation.[119] By contrast, high reliability theory forbids trial-and-error learning because it is simply too risky that errors will arise.[120]

Finally, errors—including critical ones—occur constantly in the cybersecurity arena, even in entities with a strong focus on security.[121] Thus, high reliability theory does not accurately describe any known cybersecurity entities or practices. There is no role model to which to aspire. Mitigation—not prevention—must become the guiding principle.

Strangely, however, current cybersecurity proposals—in particular, proposed legislation—concentrate almost exclusively on reducing vulnerabilities rather than mitigating problems.[122] Most proposed bills (none of which have been adopted) include information sharing between firms and the government about vulnerabilities, subsidizing research into more secure technology, and monitoring networks for traffic indicative of an attack.[123] The Cybersecurity Act of 2012, for example, focused almost entirely on prevention via measures such as risk assessments, information sharing, network monitoring, and designation of critical infrastructure.[124] There were, at best, hints of efforts to reduce effects rather than prevent attacks. The bill discussed mitigation and remediation in the context of reducing vulnerabilities rather than limiting the effects of their exploitation.[125] There were no provisions whatsoever treating resilience and recovery. Similarly, the Cyber Intelligence Sharing and Protection Act, which passed in the House of Representatives in 2012, focuses entirely on sharing information about threats and risks between the public and private sectors.[126]

Executive action has similarly focused on prevention: the joint cybersecurity efforts between the United States and Canada, for example, concentrate on incident management, information sharing, and public–private partnerships.[127] President Obama's Executive Order on cybersecurity, issued

---

119 VIEGA, *supra* note 67, at 141.

120 Todd R. La Porte, *On the Design and Management of Nearly Error-Free Organizational Control Systems* (recognizing the need for "trials without error" in fields involving nuclear materials), *in* ACCIDENT AT THREE MILE ISLAND: THE HUMAN DIMENSIONS 185, 187 (David L. Sills, C.P. Wolf & Vivien B. Shelanski eds., 1982).

121 VIEGA, *supra* note 67, at 141-44.

122 Bambauer, *Conundrum*, *supra* note 26, at 607-12.

123 *Id.* at 606-12.

124 Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012). Neither this version, introduced in July 2012, nor its predecessor, introduced in February of the same year, S. 2105, 112th Cong. (2012), were enacted by Congress. *S. 3414 (112th): CSA2012*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/s3414 (last visited Mar. 22, 2014).

125 S. 3414 § 103(b)(2)(A).

126 Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2012).

127 *US, Canada Launch Joint Cybersecurity Plan*, SECURITYWEEK (Oct. 27, 2012), http://www.securityweek.com/us-canada-launch-joint-cybersecurity-plan.

after Congress failed to pass legislation addressing the issue, contemplates improving cybersecurity resilience generally.[128] However, it also concentrates entirely on vulnerability reduction, via information sharing and a voluntary best-practices framework.[129]

Finally, cybersecurity scholarship concentrates on prevention. Nathan Sales, for example, notes the importance of increasing resiliency, but focuses primarily on ways to harden systems against attacks.[130] Similarly, Deirdre Mulligan and Fred Schneider propose a public cybersecurity doctrine that considers recovery from attacks, but they concentrate on adopting a public-health model to reduce initial failures.[131] Jennifer Granick promotes information sharing as the key element to block attacks.[132] Seeking to reduce security vulnerabilities is sensible. However, failure to address mitigation precludes success, as attackers will continue to access and alter data. Thus, cybersecurity must concentrate on reducing the harm that occurs when they do so. This Article next explores why, for reducing and mitigating harms, regulation through legal mandates is necessary.

II. THE EASY CASE FOR CYBERSECURITY REGULATION

Cybersecurity is a puzzle. It has been recognized by presidential administrations of both parties as a national policy priority for fifteen years, yet there has been little progress.[133] The confluence of externalities and market failure make cybersecurity the classic case for public law regulation, but there has been little regulatory action. Why?

Cybersecurity suffers from a perfect storm of five interrelated challenges that impede regulation. First, cybersecurity regulation must confront the regulatory challenge of externalities.[134] Insecure information technology (IT) users and providers do not suffer the full costs of the harms they generate.[135] Conversely, secure users and providers do not internalize all the

---

128 Exec. Order 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013) (responding to the demonstrated "need for cybersecurity").

129 *Id.* §§ 4, 7.

130 *See generally* Sales, *supra* note 35, at 1544-67.

131 *See generally* Mulligan & Schneider, *supra* note 35, at 80-88.

132 Jennifer Granick, *How to Build Effective Cyber Defenses*, CNN (Aug. 13, 2012), http://globalpublicsquare.blogs.cnn.com/2012/08/13/how-to-build-effective-cyber-defenses.

133 Bambauer, *Conundrum*, *supra* note 26, at 591-92 (characterizing recent government efforts to define cybersecurity as "overbroad" and "expansive").

134 *See generally* Hal Varian, *System Reliability and Free Riding*, *in* ECONOMICS OF INFORMATION SECURITY, *supra* note 41, at 1.

135 *See* Sales, *supra* note 35, at 1518-19 (suggesting that governments should subsidize firms that invest in cyberdefenses).

benefits they create. Insecurity is overproduced; security is underproduced.[136] Second, information asymmetries undercut market forces that would otherwise push vendors to offer more secure products. Consumers have difficulty detecting whether firms have made improvements to cyber defenses, leading to reluctance to pay a security premium.[137] Third, cybersecurity exemplifies the difficulties of public choice theory: burdened parties have a concentrated interest in diluting or blocking regulation, while benefited ones have an amorphous interest that leads to their political disengagement.[138] Fourth, cybersecurity suffers from a collective-action problem. Benefited parties cannot coordinate effectively to compensate burdened ones, even though doing so would increase social welfare.[139] Finally, regulators have demonstrated an ingrained reluctance to impose mandates on the technology sector[140] except where such mandates allow law enforcement authorities access to communications platforms.[141] This attitude derives from concerns about information asymmetry between regulators and regulated entities,[142] the risk of regulation quickly becoming obsolete, and the cost burdens of poorly tailored mandates.[143]

This Part performs four tasks. First, it highlights the immense scope of the cybersecurity problem by demonstrating that many security challenges

---

136 *See* L. Jean Camp & Catherine Wolfram, *Pricing Security: A Market in Vulnerabilities*, *in* ECONOMICS OF INFORMATION SECURITY, *supra* note 41, at 17, 17-22.

137 *See* Carl E. Landwehr, *Improving Information Flow in the Information Security Market: DOD Experience and Future Directions*, *in* ECONOMICS OF INFORMATION SECURITY, *supra* note 41, at 155, 162-63.

138 *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION 43-52 (1965).

139 *See* Guy Halfteck, *Legislative Threats*, 61 STAN. L. REV. 629, 700 (2008) (advocating organizations' role in eliminating this collective-action problem by "ensuring group-wide compliance").

140 *See, e.g.*, Bambauer, *Conundrum*, *supra* note 26, at 607-09 (describing the Obama Administration's position that regulatory mandates related to cybersecurity are a "last resort"); Jeffrey A. Eisenach, *Spectrum Reallocation and the National Broadband Plan*, 64 FED. COMM. L.J. 87, 90-94 (2011) (noting benefits of flexibility and market forces in telecommunications policy); Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 355, 360-65 (2010) (discussing the FTC's evolving stance on regulatory efforts aimed at protecting privacy over the Internet).

141 *See* Declan McCullagh, *FBI: We Need Wiretap-Ready Web Sites—Now*, CNET (May 4, 2012), http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now (discussing FBI efforts to obtain even greater leeway to monitor websites and Internet service providers).

142 *See* REASON, *supra* note 116, at 171-75; Alan Devlin, Michael Jacobs & Bruno Peixoto, *Success, Dominance, and Interoperability*, 84 IND. L.J. 1157, 1194-95 (2009) (noting problems created by information asymmetries between regulators and market participants when regulators attempt to impose "reasonable" prices). *See generally* Jeffrey T. Macher, John W. Mayo & Jack A. Nickerson, *Regulator Heterogeneity and Endogenous Efforts to Close the Information Asymmetry Gap*, 54 J.L. & ECON. 25 (2011).

143 *See generally* Derek E. Bambauer, *Rules, Standards, and Geeks*, 5 BROOK. J. CORP. FIN. & COM. L. 49 (2011).

remain unsolved. Second, it builds the case for regulation of cybersecurity via public law. Third, it delves into the failure of existing models of regulation, such as voluntary certification, self-regulation, information sharing, designation of critical infrastructure, and education. Finally, it argues that law must step into the breach.

A. *A Series of Porous Tubes*

Cybersecurity is a significant, unsolved problem for lawyers and computer scientists alike. In 2011 and 2012 alone, the Dutch certificate authority, DigiNotar, and the American certificate authority, Comodo, were hacked, and the attackers were able to create fake cryptographic certificates for domains such as google.com and skype.com.[144] The false credentials were likely used to spy on Iranian political dissidents.[145] In 2011, Sony's PlayStation Network was hacked, exposing the personal information of 77 million users.[146] While Sony reported that users' credit card data was encrypted, their passwords were not, placing customers who reused passwords on other sites at risk.[147] The Flame malware targeting Iranian computers and networks employed a previously unknown cryptographic attack to generate false digital certificates that let it masquerade as a security update from Microsoft.[148] Google's Chrome browser, which attempts to operate within a secure "sandbox," limiting its interaction with a user's computer, was successfully hacked three times by coders who employed zero-day vulnerabilities against the software.[149] A server configuration error allowed an attacker from Eastern Europe to gain access to personal information for

144 Jeremy A. Kaplan, *Could DigiNotar Hack Lead to a Cyberattack on You?*, FOX NEWS (Sept. 6, 2011), http://www.foxnews.com/scitech/2011/09/06/hacked-turkish-business-diginotar-could-spell-disaster-for; Steve Schultze, *DigiNotar Hack Highlights the Critical Failures of Our SSL Web Security Model*, FREEDOM TO TINKER (Sept. 6, 2011), https://freedom-to-tinker.com/blog/sjs/diginotar-hack-highlights-critical-failures-our-ssl-web-security-model; Report of Incident on 15-MAR-2011, COMODO http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html (last visited Mar. 22, 2014).

145 *See* sources cited *supra* note 144.

146 Shane Richmond & Christopher Williams, *Millions of Internet Users Hit by Massive Sony PlayStation Data Theft*, TELEGRAPH (Apr. 26, 2011), http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html; *Sony Faces Legal Action over Attack on PlayStation Network*, BBC NEWS (Apr. 28, 2011), http://www.bbc.com/news/technology-13192359.

147 Ned Potter, *Sony PlayStation Network Hacked Again, Closes 93,000 Accounts*, ABC NEWS (Oct. 12, 2011), http://abcnews.go.com/blogs/technology/2011/10/sony-playstation-network-hacked-again-closes-93000-accounts.

148 *See* Mathew J. Schwartz, *Flame Malware Tapped World Class Crypto*, INFORMATIONWEEK (June 8, 2012), http://www.informationweek.com/news/security/management/240001763.

149 Dan Goodin, *At Hacking Contest, Google Chrome Falls to Third Zero-Day Attack*, ARS TECHNICA (Mar. 9, 2012), http://arstechnica.com/business/2012/03/googles-chrome-browser-on-friday.

780,000 Utah residents, at least 280,000 of whom had their Social Security numbers stolen.[150] The hacking collective Anonymous broke into local law enforcement systems and posted sensitive information (e.g., Social Security numbers and bank account numbers) to the Internet.[151] Payment processor Global Payments suffered a data breach that exposed 1.5 million credit card numbers and account details.[152] A New York State utility suffered unauthorized access to the records of up to 1.8 million customers, including payment data and Social Security numbers.[153]

These examples of recent attacks are merely representative; cybersecurity problems are legion. Networked computer systems are massively insecure. This insecurity is neither negligence nor accident; it is a systemic problem of information technology. Why has cybersecurity remained so lax, and why have efforts to pass legislation to address its challenges consistently failed?

B. *Root Causes*

Cybersecurity presents four characteristics that challenge regulation: externalities, information asymmetries, public choice problems, and technological timidity.

1. Externalities

Cybersecurity vulnerabilities persist not merely because networked computing is complex, but because cybersecurity is a classic example of how externalities challenge regulation.[154] Google, Microsoft, and even end users fail to internalize the insecurity costs they create, thereby generating a negative externality.[155] Even industries such as the retail-payments sector,

---

150 *See* Nicole Lewis, *Utah's Medicaid Data Breach Worse than Expected*, INFORMATIONWEEK (Apr. 11, 2012), http://www.informationweek.com/news/healthcare/security-privacy/232900128.

151 *See* Damon Poeter, *Anonymous Hack of Texas Police Contains Huge Amount of Private Data*, PCMAG (Sept. 6, 2011), http://www.pcmag.com/article2/0,2817,2392522,00.asp; Ujala Sehgal, *Anonymous Retaliates Against Arrests with Massive Police Hack*, ATLANTIC WIRE (Aug. 6, 2011), http://www.theatlanticwire.com/technology/2011/08/anonymous-retaliates-against-arrests-massive-police-hack/40924.

152 *Global Payments Says Data Breach Is "Contained,"* REUTERS (June 12, 2012), http://www.reuters.com/article/2012/06/12/us-globalpayments-breach-idUSBRE85B1IC20120612.

153 Mike Lennon, *New York State Electric & Gas and Rochester Gas and Electric Suffer Data Breach*, SECURITY WEEK (Jan. 23, 2012), http://www.securityweek.com/new-york-state-electric-gas-and-rochester-gas-and-electric-suffer-data-breach.

154 *See* Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610, 610 (2006) (noting that most Internet users "do not bear the full consequences" of joining the network); Sales, *supra* note 35, at 1519-21 (conceding that most companies do not consider the cost of externalities).

155 *See* Sales, *supra* note 35, at 1519-21.

where firms face significant financial and legal risk for cybersecurity failures, are characterized by pervasive externalities.[156] Consider two examples: the vendor and the user. The vendor produces software employed by users. If there is a security flaw in that software, and if the flaw is exploited, the user is likely to suffer harm in the form of compromised data or improper software functioning.[157] A Windows vulnerability could permit an attacker to view financial data stored on a user's computer or enlist that computer in a botnet[158] that sends spam to others. Microsoft—the vendor—is virtually immune from liability for these failures, even if the flaw existed due to the company's negligence.[159] End-user license agreements typically disclaim all liability on the vendor's part, and tort law has failed to impose a duty of care on software manufacturers.[160] Indeed, software is unusual in this regard.[161] Thus, Microsoft causes harm for which it does not bear the cost; consequently, the company does not factor those harms into its investment decisions regarding security precautions.[162]

Similarly, a user may fail to take adequate security precautions (such as by continuing to use an out-of-date web browser or neglecting to install patches for her computer's operating system).[163] These failures create risks to others: her computer may become part of a botnet that sends spam or launches denial-of-service attacks, or a virus may send copies of itself to everyone in her email program's address book.[164] Those affected have little redress: their relationships with the users may not have contractual bases for allocating risk; it may be difficult to quantify their harms for recovery in tort; tort doctrine may not impose a duty to third parties; or, it may be

---

156 *See* Mark MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 3, 22-24 (describing various costs associated with security breaches).

157 *See* Camp & Wolfram, *supra* note 136, at 18-22; Sales, *supra* note 35, at 1519-21.

158 A botnet is a set of computers that have been infected with malware and that are controlled by someone other than their users. Botnets are often used for crimes such as spamming and denial of service attacks. Mindi McDowell, *Security Tip (ST06-001): Understanding Hidden Threats: Rootkits and Botnets*, US-CERT, http://www.us-cert.gov/ncas/tips/ST06-001 (last revised Feb. 6, 2013).

159 See Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 426-27 (2008).

160 *Id.* at 450-57.

161 Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 PITT. J. TECH. L. & POL'Y 1, 88-89 (advocating liability for vendors of flawed software).

162 Scott, *supra* note 159, at 484.

163 *See, e.g.*, *Cybersecurity Must Focus on Users, Not Just Attackers*, TECHJOURNAL (Nov. 29, 2011), http://www.techjournal.org/2011/11/cyber-security-must-focus-on-users-not-just-attackers (suggesting that educating users about risks and defense strategies could aid prevention of future attacks).

164 *See* Richard Clayton, *Might Governments Clean-up Malware?*, 81 COMM. & STRATEGIES 87, 89-90 (2011).

difficult to identify the insecurity's source.[165] Like the vendor, the user will underinvest in security, because she does not bear the full costs of insecurity.

Conversely, those who are secure fail to internalize the benefits of operating safely. Secure users and vendors create positive externalities for which they cannot charge beneficiaries.[166] This is similar to the "herd immunity" effect observed in populations vaccinated for diseases: an immunized person benefits personally by not contracting the malady and benefits others by not acting as a vector for their infection.[167] Positive externalities may lead to underinvestment in the relevant behavior. One can view cybersecurity as a public good: secure firms create a boon that benefits all other connected users (making it nonrivalrous), since those users do not suffer attacks launched from those companies' computers, and it is practically impossible to confine those benefits only to paying customers (making it nonexcludable).[168] Security precautions are costly, and positive externalities diminish the benefit to offset these costs. Thus, both positive and negative externalities cause cybersecurity to be underproduced.

2. Information Asymmetries

Information asymmetries also impede achievement of greater cybersecurity. Users have difficulty evaluating the veracity of companies' claims regarding security in their products.[169] Partly, this is because firms do not know the full extent of their software's vulnerabilities, as demonstrated by the growing wave of zero-day attacks.[170] Also, firms have pecuniary incentives to send inaccurate signals to consumers regarding security.[171] Claims about

---

165 Camp & Wolfram, *supra* note 136, at 18-22.

166 *Id.* at 19.

167 Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 64 (2005); Sales, *supra* note 35, at 1540-41.

168 *See generally* Michel van Eeten & Johannes M. Bauer, *Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications*, 17 J. CONTINGENCIES & CRISIS MGMT. 221, 230 (2009). For background on nonrivalrous and nonexcludable goods, see *Public Goods*, U. PITTSBURGH, http://www2.pitt.edu/~upjecon/MCG/MICRO/GOVT/Pubgood.html (last visited Mar. 22, 2014).

169 *See* Anderson & Moore, *supra* note 154, at 610 ("Insecure software dominates the market for the simple reason that most users cannot distinguish it from secure software; thus, developers are not compensated for costly efforts to strengthen their code.").

170 *See generally* Kim Zetter, *Sleuths Trace New Zero-Day Attacks to Hackers Who Hit Google*, WIRED (Sept. 7, 2012), http://www.wired.com/threatlevel/2012/09/google-hacker-gang-returns (discussing "the Elderwood Gang" of hackers and the "remarkable . . . number of zero-day vulnerabilities they have burned through in the last three years").

171 Landwehr, *supra* note 137, at 162-63.

software security are difficult to verify or disprove.[172] Rational vendors will accordingly skimp on security investments, at least at the margins, since they will likely not be able to recover those costs via higher prices that correlate with higher quality.[173] Thus, consumers face a problematic information asymmetry when deciding on software purchases.

A common response to this information gap is to rely on trusted third parties as certifiers.[174] Unfortunately, certifiers are vulnerable to capture. Harvard Business School professor Ben Edelman showed that websites certified by TRUSTe were twice as likely to be insecure as uncertified sites.[175] TRUSTe's inspections were not rigorous, leading to adverse selection: less secure sites were more likely to seek certification, generating a false signal to consumers.[176] Since TRUSTe's revenues derived from sites applying for certification, the company had an incentive to grade security generously. This risk applies to software as well: firms could even set up sockpuppet certifiers that they control—a result similar to "greenwashing" and environmental certification.[177] Security thus embodies a market failure driven by two information problems: the difficulty of ascertaining an accurate reading of software's security, and incentives to fill this gap with false signals.[178]

---

172 *See* Ragnar Schierholz & Kevin McGrath, *Security Certification—A Critical Review* 3 (paper presented at the 2010 Indus. Control Sys. Joint Working Grp. Fall Conference), *available at* ftp://ftp.sei.cmu.edu/pub/pruggiero/ics-cert/1/Security_Certification-A_critical_review_2010-10-06-ICSJWG_Remediated.pdf (last visited Mar. 22, 2014) ("Security properties of a software product are a quality dimension which is difficult to assess . . . prior to purchase, at least not at justifiable cost.").

173 *See, e.g.*, Douglas A. Barnes, Note, *Deworming the Internet*, 83 TEX. L. REV. 279, 292-93 (2004) (discussing the "lemons equilibrium," where "sellers can produce low-quality goods that buyers cannot distinguish from high-quality goods").

174 *See generally* Lesley K. McAllister, *Regulation by Third-Party Verification*, 53 B.C. L. REV. 1, 47-52 (2012) (discussing third-party verification schemes including accreditation rules, verification performance rules, and reporting and disclosure rules).

175 *See* Benjamin Edelman, *Adverse Selection in Online "Trust" Certifications*, ELECTRONIC COM. RES. & APPLICATIONS, Jan.–Feb. 2011, at 17, 20 ("Only 94.6% of TRUSTe-certified sites are actually trustworthy[,] . . . whereas 97.5% of non-TRUSTe sites are trustworthy.").

176 *See id.* at 20 (indicating that TRUSTe's results confirm the adverse selection posited, where a trust authority produces a favorable initial reputation, but later "untrustworthy firms can profit from certification").

177 *See generally* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 440 (2009) ("Greenwashing . . . occurs when companies recognize that reputation in an area such as environmental practices motivates economic decisions by consumers."); Miriam A. Cherry & Judd F. Sneirson, *Beyond Profit: Rethinking Corporate Social Responsibility and Greenwashing After the BP Oil Disaster*, 85 TUL. L. REV. 983, 999-1009 (2011) (discussing BP's efforts to "green its image").

178 *See generally* Schierholz & McGrath, *supra* note 172 (listing various "[s]hortcomings of [e]xisting [s]ecurity [c]ertifications," including "[c]ertification criteria," "[a]dverse selection," and "[m]oral [h]azard").

3. Public Choice Problems

Cybersecurity also presents a classic public choice problem.[179] Firms facing potential burdens of regulation have a concentrated pecuniary interest in avoiding such regulation.[180] These companies possess the resources to lobby legislators and regulators: they are politically sophisticated and are repeat players in the regulatory game.[181] By contrast, while consumers benefit from increased cybersecurity in regulated firms, they have diffuse, uncertain interests that impede advocating for change.[182] The benefits to each individual vary. Some people, such as those who avoid identity theft as a result of enhanced security, would receive significant utility from the change, while others would receive little or none. It is difficult, if not impossible, for individuals to know ex ante how much benefit they would derive from greater cybersecurity.[183] This makes them less likely to press for regulation that could benefit them: lobbying or political action would impose real, predictable costs for an ephemeral future benefit. This imbalance pushes them toward inaction.

Organizations that would have to expend resources to comply with cybersecurity regulation have a significant, immediate incentive to resist it, and they possess the knowledge and finances to do so. They are counterbalanced weakly, if at all, by those who would benefit. The pattern of American (in)action on cybersecurity legislation fits this model perfectly. Even bills that have been proposed in Congress have been minimalist in their mandates, focusing on information sharing, allocation of responsibility among federal agencies, and voluntary measures or self-regulation.[184] Indeed, the only bill with any substantive regulatory provisions—the Cybersecurity Act of 2012—failed due to opposition to its requirement that operators of critical infrastructure implement government-generated security standards.[185] The revised

---

179 *See generally* OLSON, *supra* note 138, at 43-52 (explaining how different-sized groups relate differently to collective goods).

180 *See generally* James J. Park, *Rules, Principles, and the Competition to Enforce the Securities Laws*, 100 CALIF. L. REV. 115, 127 (2012) ("When private interests capture public enforcers the result might be underenforcement.").

181 *See generally* Daniel A. Farber & Philip P. Frickey, *The Jurisprudence of Public Choice*, 65 TEX. L. REV. 873, 883-90 (1987) (describing interest groups' behavior in the political process).

182 *See id.* at 892 ("The 'free rider' problem suggests that it should be nearly impossible to organize large groups of individuals to seek broadly dispersed public goods.").

183 *See generally supra* subsection II.B.2.

184 *See* Bambauer, *Conundrum*, *supra* note 26, at 607-09 (noting that "proposals to use law to improve cybersecurity have been strikingly minimalist").

185 Ellen Nakashima, *Senate Ready to Take Up Cybersecurity Bill that Critics Say Is Too Weak*, WASH. POST, July 25, 2012, at A2 (noting how "business interests, which have powerful influence in the Senate," opposed the Act).

version, introduced in the summer of 2012, made those standards optional but still faced industry opposition.[186] The public choice dynamic of cybersecurity makes regulation less likely and, if it does occur, less comprehensive.

4. Technological Timidity

Regulators have been reluctant to engage in substantive IT regulation.[187] Legislative mandates for IT can be grouped roughly into two camps: generalized goals and process requirements. First, legislation specifies a general goal and leaves implementation details to the regulated entity. For example, the Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires that telecommunications service providers and equipment manufacturers provide a means for law enforcement to monitor information that travels across their networks or equipment.[188] This is a narrow, specific, and manageable goal: telecommunications providers and vendors must give law enforcement a single point for wiretapping.

Second, the legal rules set a process-based requirement: the regulated entity must engage in analysis, detail its method for addressing the problem, and undergo periodic assessment of its implementation of a solution.[189] One example is the requirements for publicly traded companies of section 404 of the Sarbanes–Oxley Act of 2002.[190] Firms must document their internal controls for financial reporting, including those reliant on information technology, and then demonstrate to their auditors' satisfaction that they have implemented those controls.[191] Auditors must document the controls and make that documentation publicly available.[192] Further, corporate officers must attest to the accuracy of the auditors' documentation or face

---

186 *See generally* Megan Geuss, *Senate Introduces Revised Version of Cybersecurity Act of 2012*, ARS TECHNICA (July 19, 2012), http://arstechnica.com/tech-policy/2012/07/senate-introduces-revised-version-of-the-cybersecurity-act-of-2012 (describing the July 2012 revisions to the Act); Nicole Henderson, *Noise Filter: Revised US Cybersecurity Act Still Has Problems*, WHIR (July 24, 2012), http://www.thewhir.com/web-hosting-news/noise-filter-revised-us-cybersecurity-act-still-has-problems (noting opposition to the Cybersecurity Act from Computing.co.uk and the Electronic Frontier Foundation).

187 *See, e.g.*, Rob Frieden, *Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanization*, 3 VA. J.L. & TECH. 8, paras. 30-48 (1998) (discussing the government's limited responses to problems of Internet access).

188 47 U.S.C. § 1002(a) (2006).

189 *See, e.g.*, 15 U.S.C. § 7262 (2012) (requiring annual reports and assessments from public accounting firms); 44 U.S.C. § 3543 (2006) (detailing functions that the Director of the Central Intelligence Agency must assume in monitoring others' information-security measures).

190 *See* 15 U.S.C. § 7262(a) (requiring, inter alia, an annual "internal control report").

191 *Id.*

192 *Id.* § 7262(b).

criminal penalties.[193] The Sarbanes–Oxley Act sets no substantive guidelines for the sufficiency of internal controls. Rather, it defers to the private information of traded companies and their auditors to ensure that appropriately tailored safeguards are in place.

Similarly, the Financial Services Modernization Act of 1999 (commonly known as the Gramm–Leach–Bliley Act (GLBA)) and its implementing regulations, which apply to financial institutions, mandate that regulated firms adopt measures to protect customers' personal information.[194] Rather than specify what measures suffice, the GLBA requires that firms assess the risks they face, design a set of countermeasures, implement it, test it, and adjust the countermeasures as circumstances change.[195] While regulators such as the Federal Trade Commission provide suggestions and guidance on best practices, GLBA requirements focus on a process that tailors safeguards to each firm, rather than specifying top-down mechanisms.[196] The GLBA is widely considered the success story of federal cybersecurity regulation, but it too is deferential to individualized judgments by each firm.[197] The GLBA, like section 404 of the Sarbanes–Oxley Act, places its faith in process-driven solutions, and expresses skepticism toward regulators' ability to specify what measures firms should take to accomplish legislative goals.

Both approaches evince regulatory wariness regarding specific security commands. This technological timidity has at least three roots. First, scholars note the asymmetry in information between the regulators and the regulated.[198] This can make regulation inefficient, and perhaps ineffective: it fails to adjust for the individual circumstances, risks, and requirements of

---

193 *Id.* § 7241(a); *see also* Press Release, U.S. Sec. & Exch. Comm'n, Commission Proposes Amendments Regarding CEO, CFO Certification Under Sarbanes–Oxley (Mar. 21, 2003), http://www.sec.gov/news/press/2003-39.htm.

194 *See generally* 12 U.S.C. § 1811 (2012) (outlining provisions of the Act); 15 U.S.C. § 6805 (listing the various financial institutions governed by the Act); 16 C.F.R. §§ 314.1–314.5 (2013) (setting forth implementing regulations for the Act).

195 *See* 16 C.F.R. § 314.3 ("You shall develop, implement, and maintain a comprehensive information security program.").

196 *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, BUREAU OF CONSUMER PROTECTION BUSINESS CENTER (Apr. 2006), http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule (outlining requirements for compliance with the Act).

197 *See generally* Sales, *supra* note 35, at 1538-39 ("[F]inancial institutions will tend to prioritize defense against the one form of intrusion singled out by their regulators . . . .").

198 *See, e.g.*, Paul Rosenzweig, *Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?*, 8 I/S: J.L. & POL'Y FOR INFO. SOC'Y 388, 400 (2012) (discussing the potential for individuals to compete with established institutions); Howard A. Shelanski, *Justice Breyer, Professor Kahn, and Antitrust Enforcement in Regulated Industries*, 100 CALIF. L. REV. 487, 490-91 (2012) ("[T]he information necessary . . . is in the hands of the very companies being regulated.").

targeted firms.[199] Thus, firms may waste resources complying with mandates when they could achieve the same ends at a lower cost if not limited by government regulation. Second, on a less generous accounting of firms' motives, regulated entities may engage in strategic behavior, revealing information to regulators only when it benefits them and concealing it otherwise.[200] Telecommunications regulation is replete with cautionary tales of this sort, such as the dialectic between the Federal Communications Commission (FCC) and carriers who were required to provide access to parts of their networks to competitors at cost, but where that cost information was under the control of the carriers.[201] Unsurprisingly, carriers manipulated the information to increase apparent cost.[202] Finally, there are regulatory costs. Requirements need to be updated, and regulators must expend efforts to accumulate information and adjust mandates.[203] This set of worries explains the strong preference for standards rather than rules in regulating technology.[204] Regulators fear the pace of technological change and face protests from regulated entities that specific mandates will be rapidly outdated, costly, and inefficient. This pushes them either to specify goals but be agnostic about means, or to enshrine process over ends—neither of which is effective for cybersecurity.

In short, for all of these reasons, the structural dynamic of cybersecurity is tilted heavily against regulation.

C. *Failed Patches*

Alternatives to regulatory mandates have failed to improve cybersecurity.[205] Thus far, moves to improve cybersecurity have relied principally on using code to fight code, educating the public about cybersecurity precautions, sharing information about threats and weaknesses, and creating market

---

199 *Shelanski*, *supra* note 198, at 491 ("[R]egulation is . . . usually slow to adapt to new market conditions.").

200 *See* John D. Graham, *Saving Lives Through Administrative Law and Economics*, 157 U. PA. L. REV. 395, 510-11 (2008) ("There are well-documented cases where . . . overstatement has occurred.").

201 Howard A. Shelanski, *The Case for Rebalancing Antitrust and Regulation*, 109 MICH. L. REV. 683, 722-25 (2011) (discussing the FCC's experience with access regulation).

202 *See* Verizon Commc'ns Inc. v. FCC, 535 U.S. 467, 486 (2002) (discussing how an information advantage allowed utilities to "manipulate the rate base and renegotiate the rate of return every time a rate was set").

203 *See* Bambauer, *Rules, Standards, and Geeks*, *supra* note 143, at 52-53 (discussing the administrative costs of rule-based regulation).

204 *Id.*

205 *Cf.* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 675-76 (1998) (arguing that "a series of methodological gaps . . . must be filled" to understand regulatory interventions and "order the architecture of cyberspace").

incentives for security. Few of these methods have had any effect. And the ones that have worked have not worked well.

1. Fighting Code with Code

Since vulnerabilities in software code are the heart of the cybersecurity problem, current efforts concentrate heavily on improving code in four primary ways: to improve the security of software and hardware with secure development efforts,[206] to block attacks with firewalls and antivirus systems,[207] to spot attacks with intrusion detection systems,[208] and to recover from such attacks with backup and recovery software.[209] While each has helped, none has succeeded completely. Moreover, even when code-based solutions exist, they require deployment to function.[210] This problem recalls the issues with cybersecurity externalities discussed above: users and firms have inadequate incentives to implement patches and other security measures. Reconfiguring those externalities requires measures outside of code.

One controversial code-based proposal would aid private-sector efforts by having the government monitor for attacks.[211] This plan faces an underappreciated conflict of interest. The National Security Agency (NSA) has developed an intrusion detection system named "Einstein" to monitor government networks for intrusion.[212] The first two Einstein versions concentrated on disseminating security information and detecting malicious code such as viruses.[213] Version 3 is broader in two dimensions. First, it offers active capabilities—Einstein 3 can interdict malicious activity, not just

---

206 *See, e.g.*, BASTILLE LINUX, http://www.bastille-linux.org (last visited Mar. 22, 2014); *Microsoft Security Dev. Lifecycle*, MICROSOFT, http://www.microsoft.com/security/sdl/default.aspx (last visited Mar. 22, 2014).

207 *See, e.g.*, VIEGA, *supra* note 67, at 55-63; Tony Northrup, *Firewalls*, MICROSOFT TECHNET, http://technet.microsoft.com/en-us/library/cc700820.aspx (last visited Mar. 22, 2014).

208 *See, e.g.*, Damiano Bolzoni & Sandro Etalle, *Approaches in Anomaly-Based Network Intrusion Detection Systems*, *in* INTRUSION DETECTION SYSTEMS 1 (Roberto Di Pietro & Luigi V. Mancini eds., 2008).

209 *See generally* W. CURTIS PRESTON, BACKUP & RECOVERY (2007).

210 VIEGA, *supra* note 67, at 221-22.

211 *See* Mark D. Young, *United States Government Cybersecurity Relationships*, 8 I/S: J.L. & POL'Y FOR INFO. SOC'Y 277, 310-12 (2012) (describing the public–private partnership between the National Institute of Standards and Technology (NIST) and the NSA).

212 Marc Ambinder, *Cyber Security: Einstein and the Privacy Debate*, ATLANTIC (Sept. 21, 2009), http://www.theatlantic.com/politics/archive/2009/09/cyber-security-einstein-and-the-privacy-debate/26906.

213 Ben Bain, *DHS Releases New Details on Einstein 3 Intrusion Prevention Pilot*, FCW (Mar. 19, 2010), http://fcw.com/articles/2010/03/19/einstein-3-test-intrusion-prevention-system.aspx.

monitor it.[214] Second, the government has suggested deploying Einstein 3 to private network operators, such as AT&T, to monitor government traffic on their systems.[215]

This proposal has raised concerns about privacy and civil liberties.[216] Even casting those concerns aside, however, allowing the NSA to monitor civilian networks will likely offer fewer cybersecurity benefits than expected. To understand why, recall the story of the attack on Coventry, England. On the night of November 14, 1940, the German Air Force raided this British industrial city.[217] Over 400 bombers dropped 500 tons of bombs on the city, destroying much of it and killing 568 people.[218] Prime Minister Winston Churchill may have known about the attack ahead of time.[219] The cryptographers at Bletchley Park had broken the German cipher implemented via the famous Enigma machines.[220] A British intelligence officer claims to have delivered information that Coventry would be the target of the raid to Churchill several hours before the attack.[221] Churchill, on this theory, made an agonizing choice: he sacrificed Coventry's citizens to protect Britain's codebreaking ability. If he had evacuated Coventry, or augmented its air defenses, the Germans might have suspected that their communications were compromised.[222]

---

214 *DHS to Begin Deployment of Einstein 3 System This Year*, INFOSECURITY (Jan. 28, 2011), http://www.infosecurity-magazine.com/view/15536/dhs-to-begin-deployment-of-einstein-3-system-this-year.

215 Kim Zetter, *NSA Shields Government Networks with More AT&T Secret Rooms*, WIRED (July 6, 2009), http://www.wired.com/threatlevel/2009/07/einstein. *See generally* U.S. DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INITIATIVE THREE EXERCISE (2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf (discussing an exercise to demonstrate the Einstein technology suite).

216 *See generally* Steven M. Bellovin et al., *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure*, 3 HARV. NAT'L SECURITY J. 1 (2011) (discussing the various technical and policy concerns with extending Einstein 3).

217 *15 November, 1940: Germans Bomb Coventry to Destruction*, BBC: ON THIS DAY, http://news.bbc.co.uk/onthisday/hi/dates/stories/november/15/newsid_3522000/3522785.stm.

218 *See generally* F.W. WINTERBOTHAM, THE ULTRA SECRET 60 (1974); Tony Rennell, *Did Churchill Annihilate Coventry to Protect an Even Bigger Prize?*, DAILY MAIL, http://www.dailymail.co.uk/home/article-1004223/Did-Churchill-annihilate-Coventry-protect-bigger-prize.html (last updated Apr. 1, 2008).

219 Ian Shoesmith & Jon Kelly, *The Coventry Blitz 'Conspiracy*,' BBC NEWS (Nov. 12, 2010), http://www.bbc.co.uk/news/uk-11486219. *See generally* Anthony D'Amato, *Legal and Moral Dimensions of Churchill's Failure to Warn*, 20 CARDOZO L. REV. 561 (1998) (arguing against Churchill's decision not to provide Coventry early warning of the attack).

220 *See* SIMON SINGH, THE CODE BOOK 160-89 (1999).

221 Shoesmith & Kelly, *supra* note 219.

222 *See* SINGH, *supra* note 220, at 184-85 (discussing the precautions taken by the Allies before putting decoded intelligence to use).

Other historians dispute this allegation and argue that Churchill knew of the raid, but not its target.[223] Regardless whether it accurately describes the night of November 14, the Coventry story illustrates the difficulties with NSA monitoring of civilian networks. If the NSA detects traffic that demonstrates a zero-day attack, it faces a quandary. Should the NSA help the target deflect the attack, the attacker will know that the defenders, too, know of that vulnerability.[224] They will suspect—probably correctly—that the United States has tools to exploit the vulnerability. Thus, the NSA must choose between offense and defense—between the two halves of its organization.[225] If they help ward off the attack, they may sacrifice a cyberweapon in their arsenal. But if they choose to preserve their own exploit code, the government must allow the malicious traffic to pass—even revealing that it is an attack could compromise their secret. It is likely that the NSA will, at times, choose offense. This tension between protecting computing resources and maintaining the capacity to exploit others' vulnerabilities is inescapable and likely explains the muted calls from the NSA and other Department of Defense (DOD) branches for greater cybersecurity precautions.[226]

While code-based efforts are useful, they have plainly proven insufficient. The effort to improve cybersecurity using code itself is an arms race, and one in which the attackers have significant advantages.

2. Educating the Targets

Education and norm-based efforts have been deployed to build a culture of cybersecurity. These have come principally in two forms. The first focuses on educating users about proper computing hygiene, with particular attention to online safety.[227] The second concentrates on encouraging key entities such as Internet Service Providers (ISPs) and software vendors to

---

223 Shoesmith & Kelly, *supra* note 219.

224 *Cf.* SINGH, *supra* note 220, at 184.

225 *See Mission*, NAT'L SECURITY AGENCY / CENT. SECURITY SERVICE, http://www.nsa.gov/about/mission/index.shtml (last modified Apr. 15, 2011).

226 *See* Noah Shachtman, *Security Watch: Beware the NSA's Geek-Spy Complex*, WIRED (Mar. 22, 2010), http://www.wired.com/magazine/2010/03/st_essay_nsa (calling for the NSA to be bifurcated between the "locked-down spy division and [the] relatively open geek division").

227 *See, e.g.*, Robert LaRose, Nora J. Rifron & Richard Enbody, *Promoting Personal Responsibility for Internet Safety*, COMM. OF ACM, Mar. 2008, at 71, 74-76 (discussing the prevalence and effectiveness of individual involvement in cybersecurity); NAT'L INITIATIVE FOR CYBERSECURITY EDUC. (NICE), http://csrc.nist.gov/nice/ (last visited Mar. 22, 2013) (teaching personal cybersecurity); STAYSAFEONLINE, http://staysafeonline.org/ (last visited Mar. 22, 2013) (same).

share information about threats with each other and with the federal government.[228] Neither has proven effective.[229]

Inculcating norms of safe computing protects some people, but not nearly enough to make an appreciable difference for cybersecurity. Even careful Internet use may not provide sufficient protection. Security researcher Charlie Miller demonstrated how to "pwn"—gain unauthorized control over—an iPhone merely by persuading the phone's owner to browse a webpage containing malicious code.[230] While Apple has fixed that particular flaw, Internet users are defenseless against zero-day attacks. Precautions such as personal firewalls may not provide sufficient information for users to make decisions about permitting access to programs, and protections such as Secure Sockets Layer (SSL) encryption may give a false sense of security.[231] Users who take precautions pay an immediate cost (e.g., avoiding desirable websites or applications) for an uncertain payoff (i.e., remaining secure). Behavioral economics demonstrates that people heavily discount risks of future harm when avoiding those risks imposes present disutility.[232] Lastly, as Internet access becomes increasingly ubiquitous with the wider availability of broadband and of mobile Internet devices such as smartphones, there is a constant influx of new, uneducated users, who present an attractive target for attackers.[233] Many cyberattacks, from botnets to spam, require only a small fraction of individual attacks to succeed for the larger scheme

---

228 *See, e.g.*, Department of Defense (DOD)–Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 32 C.F.R. pt. 236 (2013) (protecting classified DOD information transmitted by the defense industry); *About Us*, MULTI-STATE INFO. SHARING & ANALYSIS CENTER, http://msisac.cisecurity.org/about (last visited Mar. 22, 2014) (describing cooperation among the states and local governments to share and analyze security information); *About Us*, US-CERT INCIDENT REPORTING SYS., https://www.us-cert.gov/about-us (last visited Mar. 22, 2014) (describing a cybersecurity-incident reporting system).

229 *See, e.g.*, Van Eeten & Bauer, *supra* note 168, at 229 ("Until now, government policies have focused on user awareness campaigns, better international collaboration among law enforcement agencies, public–private information sharing and better data collection on security problems. While useful, these measures have proven to be ineffective to reduce the threats posed by botnets.").

230 Robert O'Harrow, Jr., *Cyberspace: The Fragile Frontier*, WASH. POST, June 3, 2012, at A1.

231 VIEGA, *supra* note 67, at 59-63, 171-74.

232 *See, e.g.*, Christine Jolls, Cass R. Sunstein & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1538-39 (1998) (discussing how individuals "often behave in ways at odds with conventional economic analysis, due to problems of self-control").

233 *See* Steven Furnell, Valleria Tsaganidi & Andy Phippen, *Security Beliefs and Barriers for Novice Internet Users*, 27 COMPUTERS & SECURITY 235, 236-39 (2008) (examining the lack of insight typical Internet users have regarding online security).

to work.[234] As security expert John Viega notes, "[Getting 0wned] is a lot easier than most people would expect."[235]

The second educational effort concentrates on sharing information about known threats and vulnerabilities. Information-sharing efforts have been popular among policymakers and scholars alike. President Obama's Cybersecurity Policy Review—the cornerstone of his cybersecurity program—depends heavily upon public–private partnerships and information sharing.[236] The Review contemplates "developing tailored incentives for information sharing" that could "include, as a last resort, regulatory measures as part of an integrated approach."[237] Scholars such as Gus Coldebella and Brian White worry about "structural disincentives" that create barriers to information sharing among private firms, and between private and public sector entities.[238] Economists have assessed how to structure sharing of information about security breaches given interfirm competition and heterogeneous firm characteristics.[239] Even accounting scholars seek to create incentives to bolster efficient information sharing.[240]

Legislatively, the most recent version of the Cyber Intelligence Sharing and Protection Act (CISPA), passed by the House of Representatives in April of 2013, mandates that "[t]he Director of National Intelligence . . . establish procedures to . . . share cyber threat intelligence with private-sector entities."[241] CISPA authorizes providers such as ISPs to share cybersecurity information with the government and other private entities.[242] CISPA also grants blanket immunity from liability to providers who share such information in good faith.[243] Similarly, the Senate's failed Cybersecurity Act of 2012[244]—introduced in February of 2012, but not

234 *See, e.g.*, Justin M. Rao & David H. Reiley, *The Economics of Spam*, J. ECON. PERSP., Summer 2012, at 87, 91-93 (describing the botnet method of producing spam). *See generally* Van Eeten & Bauer, *supra* note 168.

235 VIEGA, *supra* note 67, at 9.

236 *See* CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 17-29 (2010), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

237 *Id.* at 26-27.

238 Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 236-37 (2010).

239 *See generally* Esther Gal-Or & Anindya Ghose, *The Economic Consequences of Sharing Security Information*, *in* ECONOMICS OF INFORMATION SECURITY, *supra* note 41, at 95.

240 Lawrence A. Gordon, Martin P. Loeb & William Lucyshyn, *Sharing Information on Computer Systems Security: An Economic Analysis*, 22 J. ACCT. & PUB. POL'Y 461, 479-81 (2003).

241 Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. § 3 (2013).

242 *Id.*

243 *Id.*

244 *S. 2105 (112th): Cybersecurity Act of 2012*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/s2105 (last visited Mar. 22, 2014).

enacted—included provisions that would have established mechanisms for submitting reports regarding "cybersecurity threats, vulnerabilities, risks, and incidents" affecting government networks or critical infrastructure;[245] set up incentives for government employees to share information effectively;[246] authorized private entities to share "cybersecurity threat indicators" with one another;[247] directed the founding of cybersecurity threat information exchanges[248] and permitted private parties to disclose such information to the exchanges;[249] and immunized entities from liability for information sharing authorized under the Act.[250] The SECURE IT Act of 2012—introduced in March of 2012 and also not enacted[251]—contained even broader provisions that would have authorized private entities to disclose "cyber threat information" to any other entity,[252] exempted private entities from civil and criminal liability for such sharing,[253] and mandated that the federal government develop procedures for sharing this information with the private sector.[254] The DOD also moved to establish voluntary information sharing with defense contractors.[255] While none of these bills passed, the frequency with which they are introduced demonstrates that information sharing is resolutely popular. But, information-sharing norms have not worked and are not likely to. Firms have significant incentives not to disclose breaches or attacks. Revealing lapses could have reputation-related market effects. Publicly traded companies, for instance, suffer drops in share price immediately after revealing security breaches.[256] Disclosing vulnerability information risks further dissemination (even if inadvertent) that could lead to additional attacks.[257] If data is shared with the government, regulators may employ it when setting rules for, or monitoring, the firm that

245 Cybersecurity Act of 2012, S.2105, 112th Cong. § 107(d)(1).

246 *Id.* § 408.

247 *Id.* § 702(a).

248 *Id.* § 703.

249 *Id.* §§ 704–705.

250 *Id.* § 706.

251 *H.R. 4263 (112th): SECURE IT Act of 2012*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/hr4263 (last visited Mar. 22, 2014).

252 SECURE IT Act of 2012, H.R. 4263, 112th Cong. § 102(a).

253 *Id.* § 102(g).

254 *Id.* § 103.

255 Department of Defense (DOD)–Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 32 C.F.R. pt. 236 (2013).

256 *See* Huseyin Cavusoglu, Birendra Mishra & Srinivasan Raghunathan, *The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers*, 9 INT'L J. ELECTRONIC COM. 69, 94 (2004) (finding a 2.1% average decrease in market value for firms announcing Internet security breaches).

257 Gal-Or & Ghose, *supra* note 239, at 96-97.

revealed the information.[258] Finally, firms may not want to aid competitors either by reducing their information security costs or by protecting them from the same attack.[259]

More important, faith in information sharing is overdue for some skepticism. Efforts to increase information sharing assume that the information will be valuable—an often unfounded assumption. For example, the fusion centers established after the attacks of September 11, 2001, to promote information sharing about security threats have grappled continuously with an overload of inaccurate, inapposite, and generally poor-quality Suspicious Activity Reports (SARs).[260] The fusion centers have shared information that was "oftentimes shoddy, rarely timely, [and that] sometimes endanger[ed] citizens' civil liberties."[261] The U.S. Senate Permanent Subcommittee on Investigations found that the fusion centers "often produced irrelevant, useless or inappropriate intelligence reporting[,] . . . and many produced no intelligence reporting whatsoever."[262] Further, the Subcommittee was unable to identify a single instance where fusion-center reporting either identified a terrorist threat or contributed to disrupting an active terrorist plot.[263] This result occurred despite the fusion centers' allegedly central role in counterterrorism strategy.[264] The lesson for cybersecurity is clear: garbage shared is still garbage. Information-sharing efforts are popular with regulators and scholars alike; they are cheaper than technological mandates, they comport with the basic assumption that more accurate information helps markets function better, and they require little political capital. But, as with many easy things, they are not worth much.

3. Markets

Finally, though there are robust markets for cybersecurity,[265] market-driven efforts have not succeeded. Software vendors, IT consulting firms,

---

258 *Id.* at 95-96.

259 *Id.* at 96-97.

260 *See* Priscilla M. Regan & Torin Monahan, *Beyond Counterterrorism: Data Sharing, Privacy, and Organizational Histories of DHS Fusion*, INT'L J. E-POLITICS, July–Sept. 2013, at 1, 8, *available at* http://torinmonahan.com/papers/IJEP.pdf.

261 U.S. SENATE PERMANENT SUBCOMM. ON INVESTIGATIONS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 1 (2012).

262 *Id.* at 2.

263 *Id.*

264 *See id.* (quoting Department of Homeland Security Secretary Janet Napolitano as describing the centers as "one of the centerpieces of our counterterrorism strategy").

265 *Global Cybersecurity Market to Reach $61 Billion This Year*, INFOSECURITY (Jan. 30, 2012), http://www.infosecurity-magazine.com/view/23548/global-cybersecurity-market-to-reach-61-billion-this-year.

accountants, and others offer products and services intended to make information more secure. However, there are at least three structural problems with cybersecurity markets that suggest such measures are insufficient. First, externalities lead to underinvestment. Firms neither realize the total benefits of security, nor are they penalized fully for insecurity. Second, reputational effects are weak. The negative effect of data breaches upon firms' market valuation, for example, fades quickly with time.[266] And finally, markets cut both ways: there are markets for cyberweapons as well as cyberdefenses. Entities such as Vupen sell zero-day exploits on the open market (but only to friendly governments, according to Vupen).[267] There are also well-developed black markets for such information.[268] Thus, markets cannot solve the cybersecurity problem alone: informational and structural defects cause private incentives to lead to suboptimal security levels, and markets operate for attackers as well.

Nonregulatory approaches to cybersecurity simply have not worked. As Section D argues, legal mandates are necessary to fill the gap.

D. *The Need for Law*

When law specifies cybersecurity measures, security improves. While the United States has relatively few cybersecurity regulations, it does impose requirements on firms in the financial sector.[269] Banks and other financial institutions must meet the security mandates of the GLBA and regulations promulgated under it.[270] Under the GLBA, federal regulators issued joint interagency guidance on what security measures banks must adopt, and how examiners would assess compliance with them.[271] Institutions

---

266 Alessandro Acquisti, Allan Friedman & Rahul Telang, *Is There a Cost to Privacy Breaches? An Event Study* 11, 13 (Dec. 2006) (paper presented at the 27th Int'l Conference on Info. Sys.), *available at* http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=DD673F8D73246D11989046267AA29893?doi=10.1.1.207.1470&rep=rep1&type=pdf.

267 *See Vupen Exclusive and Sophisticated Exploits for Offensive Security*, VUPEN SECURITY, http://www.vupen.com/english/services/lea-index.php (last visited Mar. 22, 2014).

268 Bambauer & Day, *supra* note 43, at 1067.

269 Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.1–314.5 (2013); *see also* J. Howard Beales III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 127-28 (2008) (discussing the Safeguards Rule, 16 C.F.R. pt. 314, under the GLBA that regulates financial institutions).

270 *See generally* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 157-58 (2005) (discussing institutions' obligations under the GLBA).

271 15 U.S.C. § 6801 (2012) (codifying § 501(b) of the GLBA); *see also* Proper Disposal of Consumer Information, 69 Fed. Reg. 77,610 (Dec. 28, 2004) (codified in scattered parts of 12 C.F.R.) (implementing § 216 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681w); Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616

must undertake a risk assessment, evaluate compliance with their information security program, and review the assessment regularly.[272] The Guidelines set forth measures that financial institutions must implement, if doing so would protect customer information.[273] These include access restrictions on information systems and physical locations storing customer data, data encryption, safeguards against physical damage, monitoring to detect intrusions and response programs to mitigate unauthorized access, and procedures to ensure changes do not undercut security.[274] Some of these measures are explicitly mitigation-focused. The GLBA is designed to be flexible; it is a standard, not a rule.[275] Nonetheless, it imposes greater cybersecurity obligations on financial institutions than most firms face, and backs those requirements with federal oversight and, potentially, penalties for noncompliance.

Available empirical evidence suggests that even the GLBA's dilute mandate increases cybersecurity for financial institutions. In a study by WhiteHat Security, banking websites had the fewest average serious security vulnerabilities of any industry at 43, compared to 79 across all industries and 121 for retail sites (the industry sector with the most vulnerabilities).[276] Moreover, banks fixed the largest percentage of serious vulnerabilities of any sector, and their sites had the fewest average days of exposure to such weaknesses.[277]

Similarly, analysis of breach data from three years (2005–2007) of reports to the Identity Theft Resource Center showed that the finance and insurance industries had the lowest rate of processing errors and demonstrated a statistically significant difference in the number of breach incidents from the number expected under a random distribution.[278] Interestingly, these industries showed by far the greatest rate of misconduct by insiders leading

---

(Feb. 1, 2001) (codified in scattered parts of 12 C.F.R.) (implementing § 501(b) of the GLBA). *See generally* Thomas J. Smedinghoff, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, 16 MICH. ST. J. INT'L L. 1, 34 (2007) (describing a "process oriented legal standard" as used in the GLBA).

272 Standards for Safeguarding Customer Information, 16 C.F.R. § 314.4 (2013).

273 *Id.* § 314.3.

274 *Id.* § 314.4.

275 *See* Bambauer, *Rules, Standards, and Geeks*, *supra* note 143, at 49, 53-54 (explaining how the GLBA operates as a "purposive regulatory standard").

276 JEREMIAH GROSSMAN, WHITEHAT SECURITY WEBSITE STATISTICS REPORT 15 (2012), *available at* https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf.

277 *Id.* at 27.

278 C. Matthew Curtin & Lee T. Ayres, *Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 569, 592, 599 (2008). Processing errors occur when "normal business activity . . . lead[s] to errors that result in a loss of control over sensitive information." *Id.* at 578.

to data breaches.[279] This reinforces the idea that cybersecurity is always partial—it is not technologically possible to prevent those authorized to access data from misusing it, and other methods (such as deterrence) are imperfect as well.[280]

Finally, financial firms appear to make greater investments in security than companies in other sectors. Nathan Sales notes that banks typically invest 6%–7% of their information technology budgets in security measures.[281] He also lists specific investments that financial institutions are more likely to make than their nonfinancial counterparts, including intrusion detection systems (IDS) and smart cards.[282]

The financial sector is more secure than other industries and operates under specific cybersecurity mandates embedded in law. This correlation is no coincidence. Cybersecurity needs law. If we seek to meaningfully increase cybersecurity, we must increase legal regulation. Part III examines what legal regulation must do to address cybersecurity's negative range of access and alteration—in short, how the law can address espionage and hacking.

III. THE KNOWN UNKNOWNS

Known security bugs are *everywhere*.

Most hackers exploit known vulnerabilities. Examples are legion. The massive breach of Heartland Payment Systems occurred because the payment processor's website was vulnerable to an SQL injection attack—a widely known flaw.[283] Heartland is in good company: a study by Hewlett-Packard (HP) found that 86% of tested web applications were vulnerable to such injection attacks.[284] Sony's PlayStation Network was hacked because the company used an outdated, unpatched version of the Apache web server software.[285] Wyndham Hotels lost data on 500,000 accounts to hackers in

---

279 *Id.* at 599.

280 *See* Shawn B. Spencer, *Security vs. Privacy: Reframing the Debate*, 79 DENV. U. L. REV. 519, 520-21 (2002) (stating that "[c]entralized information is always at the mercy of dishonest or corrupt individuals willing to use it for [improper means]" and providing several examples of "abuses of centralized databases and government surveillance").

281 *See* Sales, *supra* note 35, at 1538-39 (noting that the reason for these large investments might be "[t]he unique risk of liability that banks face").

282 *Id.* at 1538.

283 JULIA S. CHENEY, HEARTLAND PAYMENT SYSTEMS: LESSONS LEARNED FROM A DATA BREACH 3-4 (2010).

284 *Web Application Vulnerabilities Decline, but Attacks Double, Says HP*, INFOSECURITY (Apr. 24, 2012), http://www.infosecurity-magazine.com/view/25329/web-application-vulnerabilities-decline-but-attacks-double-says-hp.

285 Erica Ogg, *The PlayStation Network Breach (FAQ)*, CNET (May 3, 2011), http://news.cnet.com/8301-31021_3-20058950-260; Fahmida Y. Rashid, *Sony Networks Lacked Firewall, Ran Obsolete*

Russia because their servers used default credentials and passwords and because the chain stored credit card data in plain text.[286] The SCADA systems that control many public utilities' operations often use default passwords[287]—in fact, one study found 7200 SCADA systems connected to the Internet with default passwords.[288] A significant fraction of SAP enterprise resource planning (ERP) servers are exposed to the Internet, even though the software is increasingly targeted by attacks that exploit known weaknesses.[289] The average website examined in the 2011 study contained 79 serious security vulnerabilities such as cross-site scripting weaknesses; this was actually a dramatic improvement from 2010, when the average number of flaws was 230.[290]

Remediation is slow. Companies often take nearly a year to apply patches supplied by software vendors, leaving them open to attacks.[291] Experts estimate that firms using SCADA software—including many in critical infrastructure areas such as energy utilities—only apply 10%–20% of available patches.[292] The availability of the patches indicates that solutions to these security problems are known and available to firms. Though implementing those solutions may be expensive, time consuming, or complex, it is possible. To a significant degree, users of information technology remain insecure to known unknowns—attacks against previously described and

Software: Testimony, EWEEK (May 6, 2011), http://www.eweek.com/c/a/Security/Sony-Networks-Lacked-Firewall-Ran-Obsolete-Software-Testimony-103450.

286 Paul Roberts, *FTC Sues Wyndham over Breaches Linked to $10M in Fraud*, THREATPOST (June 26, 2012), https://threatpost.com/ ftc-sues-wyndham-over-breaches-linked-10m-fraud-062612/76735.

287 *See, e.g.*, Roger A. Grimes, *Doomed by Default Passwords*, INFOWORLD (Nov. 29, 2011), http://www.infoworld.com/d/security/doomed-default-passwords-180214 (explaining that SCADA systems are particularly vulnerable because they have long depreciation schedules and run outdated versions of operating systems with publicly known exploits).

288 John E. Dunn, *Important SCADA Systems Secured Using Weak Logins, Researchers Find*, CSO (Jan. 15, 2013), http://www.csoonline.com/article/726875/important-scada-systems-secured-using-weak-logins-researchers-find.

289 *See* Alexander Polyakov & Alexey Tyurin, ERPSCAN, SAP SECURITY IN FIGURES: A GLOBAL SURVEY 2007–2011, at 31, http://erpscan.com/wp-content/uploads/2012/06/SAP-Security-in-figures-a-global-survey-2007-2011-final.pdf (finding that roughly ten percent of companies worldwide are exposed, most of which are in China).

290 *See* GROSSMAN, *supra* note 276, at 2 (noting that this figure is down from 1111 in 2007).

291 *Cf.* Sales, *supra* note 35, at 1508, 1517 (explaining this to be the case because firms do not bear the full costs of their vulnerabilities and hence have weaker incentives to fix them, and further noting that a recent study found that the electric companies surveyed took "an average of 331 days to implement security patches").

292 *See* Kelly Jackson Higgins, *The SCADA Patch Problem*, DARK READING (Jan. 15, 2013), http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240146355/the-scada-patch-problem.html (acknowledging the risk that a newly installed patch could cause an outage of the entire security system and noting that "[t]he likelihood that customers will apply patches to their SCADA systems is low").

patched vulnerabilities—by choice. As described above, this choice may be rational for each actor in purely economic terms, but it results in unacceptable levels of insecurity for society.

Building on prior work in information-based cybersecurity,[293] and applying insights from normal accident theory, this Article proposes a pair of design principles to guide regulation of the known unknowns: disaggregation and heterogeneity (or, more colloquially, "divide and differ"). The regulatory goal is for organizations to implement these principles in their computer systems. Disaggregation splits information into multiple, separated data stores. The loss of any single store, or perhaps several of them, does not confer all of an organization's information upon an attacker. Heterogeneity requires that organizations use multiple types of hardware and software: UNIX with Windows Server for operating systems, MySQL with IBM DB2 for databases, or Juniper equipment with Cisco for routers. A successful attack on any variant of hardware or software will not compromise the entire infrastructure (and hence information) for an organization.[294] In concert, these principles seek to reduce the effect of a cybersecurity failure rather than to prevent it. In normal accident theory's terms, they seek to make the system less tightly coupled.[295] They operate in parallel with efforts to reduce the likelihood of such a failure by making systems less vulnerable and by detecting and interdicting attacks when they occur. This aspect of cybersecurity—resilience—is significantly underaddressed by both scholars and policymakers.

A. *Resilience*

Disaggregation and heterogeneity increase resilience.[296] Spreading information across multiple data stores and using multiple versions of operating systems, hardware, and applications does little to prevent cyberattacks. Indeed, it may provide hackers with a greater attack surface: there are more

---

293 *See generally* Bambauer, *Conundrum*, *supra* note 26, at 587-88 (delineating an information-based, theoretical framework for cybersecurity requirements).

294 *See generally, e.g.*, DANIEL GEER ET AL., COMPUTER & COMMC'N IND. ASS'N, CYBERINSECURITY: THE COST OF MONOPOLY (2003), *available at* http://www.schneier.com/essay-318.html (discussing cybersecurity risks resulting from the dominance of Microsoft operating systems).

295 *See* PERROW, *supra* note 88, at 94-96 (discussing how coupling affects recovery from component failure).

296 *See* Kishor S. Trivedi, Dong Seong Kim & Rahul Ghosh, *Resilience in Computer Systems and Networks* (defining "resilience" in the context of computer systems as "the ability of [a]system/person/organization[] to recover/defy/resist from any shock, insult, or disturbance"), *in* PROCEEDINGS OF THE 2009 INT'L CONF. ON COMPUTER-AIDED DESIGN 74, 74-77 (2009), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=05361311.

locations for weaknesses such as misconfiguration to occur, and there are more lines of code to comb for exploits.[297] For cybersecurity scholars and policymakers fixated on stopping attacks, such an approach is anathema.

This risk-spreading approach, however, is perfectly in line with normal accident theory.[298] Inevitably, software bugs occur, and hackers discover how to exploit them.[299] There will be attacks—successful ones—against information technology systems. The key is to reduce the effects of these attacks. This lessens the harm they cause and makes hacking less attractive by reducing its payoff. Charles Perrow cites marine shipping as a similar instance where the configuration of incentives (as with cybersecurity's externalities problems) leads inexorably to accidents.[300] The approach this Article proposes, by analogy, is not to increase the vigilance of captains or the accuracy of nautical maps. It is to ensure that ships are built with watertight compartments so that an accident does not sink the vessel.[301]

The divide-and-differ strategy reduces the effects of successful attacks or breaches. The two pillars of the strategy also reinforce one another. Partitioning information into multiple repositories forces an attacker to compromise several systems to gain access to all of an organization's data.[302] This approach is particularly effective if related files—such as the plans for the Joint Strike Fighter or elements of a bank customer record—are dispersed

---

297 *See, e.g.*, Roger Grimes, *Don't Fall for the Monoculture Myth*, INFOWORLD (Apr. 24, 2009), http://www.infoworld.com/d/security-central/dont-fall-monoculture-myth-882 (explaining the flaws of the notion that one should use less-popular software because it is less likely to be attacked). *But see* Marcus J. Ranum, *The Monoculture Hype*, RANUM.COM http://www.ranum.com/security/computer_security/editorials/monoculture-hype/index.html (last visited Mar. 22, 2014) (analogizing the security of modern computer networks to that of communities of genetically diverse organisms, but noting that the analogy is not perfect—computers are not "biological entities," and several characteristics may actually lessen the danger of "monoculture").

298 *See* PERROW, *supra* note 88, at 94-95 (noting that "[s]ince failures occur in all systems, means to recovery are critical," and "[i]n loosely coupled systems there is a better chance that expedient, spur-of-the-moment buffers and redundancies and substitutions can be found").

299 *See* Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 175-79 (2008) (noting that "[t]hreats constantly evolve to exploit newly discovered vulnerabilities" and providing several examples of such sophisticated attacks).

300 *See* PERROW, *supra* note 88, at 173 (concluding that it is not a "single failure," but "the combination of system components that promotes error inducement").

301 *See* Frances Wilson, *Bad Management Helped Sink Titanic*, WALL ST. J. (Apr. 14, 2012), http://blogs.wsj.com/speakeasy/2012/04/14/how-bad-management-helped-sink-the-titanic (describing how the Titanic's builders deliberately failed to include watertight compartments in the ship's design).

302 *See generally* Bo Chen et al., *Remote Data Checking for Network Coding-based Distributed Storage Systems* 31, 31-42 (Oct. 8, 2010) (paper presented at the 17th ACM Conference on Computer & Comm. Sec.), *available at* http://dl.acm.org/citation.cfm?id=1866842.

across the data stores.[303] Then, an attacker must break into more than one system to gain access to one set of files. Employing different elements within an IT system, such as multiple operating systems, makes any single, successful attack less effective.[304] If the files are dispersed across multiple locations, each with a different code base, the attacker will need multiple exploits to gain access to or alter the data.

In normal accident theory terms, using heterogeneous systems (variegated code and hardware) makes those systems less tightly coupled.[305] A failure in one part of the system affects fewer of the other parts than if the system were homogeneous.[306] This limits the spread, and therefore the effects, of such a failure. While introducing more components into the system could make it more interactively complex, which increases the risk of error, this possibility is mitigated by disaggregation.[307] Under disaggregation, IT systems would be effectively partitioned, reducing the linkage between components in the different data stores. An exploit compromising a Windows-based computer in one data warehouse is less likely to have a spillover effect on a UNIX-based computer in a second warehouse when those two repositories are separated.[308] Thus, heterogeneity decreases system coupling and increases the complexity of system interactivity. Nonetheless, the boost in interactivity is likely offset by the disaggregation part of the known-unknowns strategy.

Splitting an organization's information into multiple parts, storing them separately, and hosting them on different software and hardware may increase the risk of a successful attack, but it greatly decreases that attack's payoff.

B. *Disaggregation: Divide and Conquer*

Disaggregation reduces the harm that accrues from a successful attack against a system by dividing data stores—information—into multiple, separate components. This reduces the payoff from a breach: a hacker gains only a fraction of the organization's information from breaking into one data

---

303 *Cf.* Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, at A1 (discussing the devastating impact of information breaches on the U.S. Air Force's fighter-jet project, but noting that the most sensitive information, stored separately, was not breached).

304 *See* NAT'L RESEARCH COUNCIL & NAT'L ACAD. OF ENG'G, TOWARD A SAFER AND MORE SECURE CYBERSPACE 107-10 (Seymour E. Goodman & Herbert S. Lin eds., 2007) (detailing techniques, including buffering and isolation, whereby information is separated from the Internet or compartmentalized to complicate attempts to breach).

305 PERROW, *supra* note 88, at 92-93.

306 *Id.* at 95.

307 *Id.* at 73-76.

308 *See id.* at 72-73.

store. Disaggregation also increases the cost of the attack: the hacker must compromise multiple systems to access the entirety of the data.

Though data storage is increasingly spread across multiple computers, such as in cloud computing, these systems are designed such that the information appears to be in one location.[309] For example, even if a database is spread across several servers in Amazon's[310] or Google's[311] cloud computing platforms, it looks like a seamless whole to users. Each part of the database is linked to, and accessible by, every other part.[312] Disaggregation breaks those links. Parts of the data store are isolated from one another, logically and perhaps physically.[313] Gaining access to one part does not confer access to any other part.

There are good examples of disaggregated systems currently in use, such as Mini-Sentinel. The Food and Drug Administration (FDA) must perform surveillance of prescription drugs after they are approved for marketing in the United States.[314] The enabling legislation requires the FDA to avoid revealing individually identifiable health information when queries are made on the resulting data.[315] To comply, the FDA built Mini-Sentinel.[316] Data sources, such as pharmaceutical companies, retain the postapproval data and structure it in standardized form.[317] Both the FDA and the data sources use Mini-Sentinel's software.[318] Queries on the data are submitted from the Mini-Sentinel Center to the data sources, which return summary

---

309 *See* Michael J. Miller, *Storing Massive Data: Distributed Data and the noSQL Movement*, PCMAG (May 4, 2012), http://forwardthinking.pcmag.com/none/297512-storing-massive-data-distributed-data-and-the-nosql-movement.

310 *See generally* Giuseppe DeCandia et al., *Dynamo: Amazon's Highly Available Key-Value Store* 205 (Oct. 16, 2007) (paper presented at the 21st ACM Symposium on Operating Sys. Principles), *available at* http://www.allthingsdistributed.com/files/amazon-dynamo-sosp2007.pdf.

311 *See generally* Sanjay Ghemawat et al., *The Google File System* 29 (Oct. 20, 2003) (paper presented at the 19th ACM Symposium on Operating Sys. Principles), *available at* http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/en/us/archive/gfs-sosp2003.pdf.

312 *Id.* (describing a file system composed of thousands of computing instances as millions of file objects).

313 *See* James Turner, *Hadoop: What It Is, How It Works, and What It Can Do*, O'REILLY STRATA (Jan. 12, 2011), http://strata.oreilly.com/2011/01/what-is-hadoop.html (describing Hadoop, a system where data is stored across "a large number of machines that don't share any memory or disks" but where results are delivered in a "unified whole").

314 21 U.S.C. § 355(k)(3) (2012). I thank Leslie Francis for this example.

315 *Id.* § 355(k)(3)(C)(i)(I).

316 Leslie P. Francis & John G. Francis, *Informatics and Public-Health Surveillance*, *in* BIOINFORMATICS LAW: LEGAL ISSUES FOR COMPUTATIONAL BIOLOGY IN THE POST-GENOME ERA 191, 204-05 (Jorge L. Contreras & A. James Cuticchia eds., 2013).

317 *Id.*

318 *Id.*

responses to queries.[319] Mini-Sentinel was designed to respond to privacy concerns, but it also provides a compelling model for security worries.[320] A breach of any single data source compromises only that entity's information. And, an attack against the querying computer at the Mini-Sentinel Center can only obtain summary information, rather than individually identifiable data.

The benefit of disaggregation—reducing the payoff of an attack and forcing an attacker to gain control over more systems—comes at two costs. First, using the data (accessing it, altering it, or both) for authorized purposes requires that the isolated parts of the information are joined, at least in part or intermittently.[321] Performing analysis on large datasets thus becomes computationally more expensive and depends on reliable connectivity between the subsets.[322]

Analysis of the divided data could occur in one of two ways. First, the system could send queries to each subset, which would process the query and return the results.[323] Under this method, the querying system would merge results from each subset. Second, the system could dynamically merge the data from the subsets, perform the query, and then store only the results.[324] While the querying entity can be a single point of failure, this risk is reduced (as with Mini-Sentinel) when it receives only summary information.[325] Under the second analytical method above, an attacker who compromises the querying computer can gain access to the entire data store. This weakness is problematic, but likely unavoidable. At a minimum, though, disaggregation can greatly reduce the number of vulnerable systems, perhaps allowing enhanced precautions to be taken with them.

Second, the disaggregated data store is (by design) less efficient than a centralized data store.[326] The system must perform more work to run tasks on the data—such as merging queries or merging parts of the information—than

---

319 *Id.*

320 *Id.*

321 *See generally* Jeffrey Dean & Sanjay Ghemawat, *MapReduce: Simplified Data Processing on Large Clusters* 137 (Dec. 6, 2004) (paper presented at the 6th Symposium on Operating Sys. Design & Implementation), *available at* http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/en/us/archive/mapreduce-osdi04.pdf.

322 Ghemawat et al., *supra* note 311, at 30.

323 Francis & Francis, *supra* note 316, at 204-05; Ghemawat et al., *supra* note 311, at 30.

324 Amazon's Simple Storage Service offers similar capabilities. AMAZON SIMPLE STORAGE SERVICE (AMAZON S3), http://aws.amazon.com/s3 (last visited Mar. 22, 2014).

325 *See* Francis & Francis, *supra* note 316, at 204-05; *cf.* Dean & Ghemawat, *supra* note 321, at 5 (discussing master failure and noting that since "there is only a single master, its failure is unlikely"); Ghemawat et al., *supra* note 311, at 33-36 (stating that a master computer could be a single point of failure due to sole control over namespace).

326 *See* Dean & Ghemawat, *supra* note 321, at 5 (discussing efforts in MapReduce, a disaggregated data storage system, to use local data whenever possible to improve efficiency).

would be necessary with seamless storage.[327] This compromise is likely tolerable given high-speed networks, processors, and disks, but it is nonetheless real.[328]

Private Manning's actions provide a compelling example of the tradeoff between the ease of analysis and the risk of compromise. Manning was able to download a trove of documents from SIPRNet, a network of sensitive but unclassified information from the Departments of Defense and State, because boundaries between different data stores had been deliberately removed.[329] After the September 11th terrorist attacks, the federal government came under criticism for "stovepiping" useful information into multiple isolated systems.[330] The intelligence community complained that these barriers prevented them from performing a comprehensive analysis to recognize patterns and from ensuring that different analysts could use relevant data and contribute insights.[331]

Manning, though, was the counterpoint. Merging data stores allowed those with access to the system—reportedly, several hundred thousand people—to view all of it.[332] Manning could thus download a massive amount of data onto an optical disc disguised as a Lady Gaga CD and then share it with the world via WikiLeaks.[333] Had the SIPRNet information remained in multiple, isolated (stovepiped) systems, Manning would have needed greater access and more time to gather the same information.

Cybersecurity is an exercise in balance. As data becomes more disaggregated, the cost of analysis rises; as it becomes more joined, the potential loss from a successful attack on it rises. Exactitude in striking this balance is impossible. The disaggregation principle, though, posits that a shift toward reducing the effects of attacks by dividing data across multiple locations is a worthwhile one. And disaggregation's benefits are increased by the second design principle—heterogeneity.

---

327 *See id.* at 6.

328 DeCandia et al., *supra* note 310, at 207-08.

329 Massimo Calabresi, *State Pulls the Plug on SIPRNet*, TIME (Nov. 29, 2010), http://swampland.time.com/2010/11/29/state-pulls-the-plug-on-siprnet.

330 *Id.*

331 *See* Michael Moran, *Tilting at "Stovepipes?"*, MSNBC (Sept. 9, 2003), http://www.today.com/id/3071393.

332 Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1519 (2012) (correlating merging data stores with access).

333 Clark Boyd et al., *Intelligence Sharing and the Danger of Leaks*, PRI'S WORLD (Nov. 30, 2010), http://www.pri.org/stories/2010-11-30/intelligence-sharing-and-danger-leaks.

C. *Heterogeneity: The Benefits of Diversity*

To increase cybersecurity, organizations should increase the heterogeneity of their computing infrastructure. Put simply, heterogeneity is diversity.[334] As with an ecosystem, there are different niches or roles in information technology systems, including servers, workstations, operating systems, and applications. Currently, economies of scale push organizations to standardize on a single product or vendor for each niche.[335] This may improve efficiency, but it worsens security.[336] Organizations should instead move in the opposite direction. For example, they should run Linux and Windows servers alongside one another and should purchase Juniper Networks routers in addition to Cisco boxes. Ideally, each part of an entity's infrastructure would be diverse—there would be no single point of failure for an attacker to exploit.

Heterogeneity posits that diversity of software and hardware decreases the expected harm from a cyberattack. Such diversity makes it more difficult for a single vulnerability or successful hack to compromise an entire system or deliver access to a complete data store.[337] Apple's MacOS is a potent exemplar.[338] Personal computers (PCs) overwhelmingly run versions of the Microsoft Windows operating system.[339] This large population of potentially vulnerable PCs attracted copious hacker attention. Macs, though, which do not run Windows-based operating systems, so far have not been attacked by such Windows bugs.[340]

---

334 *See* Justin Pope, *Biology Stirs Software "Monoculture" Debate*, BOSTON.COM (Feb. 16, 2004), http://www.boston.com/business/technology/articles/2004/02/16/biology_stirs_software_monoculture_debate (discussing the contention of some that the pervasiveness of Microsoft's "monoculture" allows a single flaw that can be exploited by a virus or the like to "wreak havoc").

335 Ryan Naraine, *IT Wrestles with Microsoft Monoculture Myopia*, EWEEK (Sept. 10, 2006), http://www.eweek.com/c/a/Windows/IT-Wrestles-with-Microsoft-Monoculture-Myopia ("The economics of standardizing still trump security headaches.").

336 GEER ET AL., *supra* note 294 ("Security dangers [are] posed by software monopolies.").

337 *Cf.* Andrew G. Haldane & Robert M. May, *Systemic Risk in Banking Ecosystems*, 469 NATURE 351, 353 (2011) ("[E]xcessive homogeneity within a financial system—all the banks doing the same thing—can minimize risk for each individual bank, but maximize the probability of the entire system collapsing.").

338 *See* VIEGA, *supra* note 67, at 105-07.

339 *See* Seth Rosenblatt, *Windows 8 Gains Market Share in December*, CNET (Jan. 3, 2013), http://reviews.cnet.com/8301-33642_7-57561974-292/windows-8-gains-market-share-in-december (reporting that the overall desktop market share for Windows operating systems was 91.74% at the end of 2012).

340 *See, e.g.*, Brian Krebs, *Experts Warn of Zero-Day Exploit for Adobe Reader*, KREBS ON SECURITY (Nov. 7, 2012), http://krebsonsecurity.com/2012/11/experts-warn-of-zero-day-exploit-for-adobe-reader ("[S]o far, they have only seen the attack work against Microsoft Windows installations of Adobe Reader.").

Even flaws in applications available on Macs, such as Adobe Acrobat, might not trouble Apple users due to the differences in coding for the two platforms.[341] Thus, an organization that uses both MacOS- and Windows-based computers would be less vulnerable to a Windows exploit than a firm that had standardized solely on Microsoft. Similarly, having a computing ecosystem that runs different operating systems, applications, and network hardware provides a useful defense against a magic bullet, such as a zero-day attack that can compromise one particular component.[342]

Heterogeneity's benefits come with costs. First, it is more expensive to operate an IT environment with multiple types of each component: there are fewer economies of scale, and there is more information to track.[343] Organizations are likely to need more IT personnel, since employees often specialize in one operating system, hardware brand, or application.[344] Second, and more important, heterogeneity increases the odds that a vulnerability will be found in the overall ecosystem and that an attacker will be able to use it.[345] With mixed operating systems, for example, an IT ecosystem is affected by both Windows and Mac bugs.

Lastly, it is likely that organizations will have difficulty diversifying certain software—in particular, custom-coded applications and ERP programs.[346] Custom applications tend to respond to unique characteristics of an organization's systems, data, and needs.[347] These individualized needs are difficult to meet with off-the-shelf software, forcing the firm either to invest in a

---

341 *Cf. id.* (noting possible limitations of the exploit).

342 *See, e.g.*, Ryan Naraine, *Microsoft Issues Word Zero-Day Attack Alert*, EWEEK.COM (Dec. 5, 2006), http://www.eweek.com/c/a/security/microsoft-issues-word-zeroday-attack-alert (reporting a cyberattack that only targeted a single Microsoft software program). In addition, it should be noted that defenses against zero-day attacks are, by definition, impossible—a zero-day is an exploitable flaw that is unknown to defenders such as vendors or antivirus makers.

343 Naraine, *supra* note 335 (noting that despite increased fears and instances of attacks targeting its programs, Microsoft remains the dominant provider of operating systems because of the economic benefits of standardization); Fred B. Schneider & Kenneth P. Birman, *The Monoculture Risk Put into Context*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2009, at 14, 14 (summarizing some of the benefits afforded by using a "monocultural" network of computer programs).

344 Schneider & Birman, *supra* note 343.

345 *See, e.g.*, *id.* at 15-16 (introducing some of the different forms a cyberattack may take).

346 *See* MICHAEL H. HUGOS & DEREK HULITZKY, BUSINESS IN THE CLOUD 94 (2010) ("Once a company makes a commitment to use an ERP system and installs the software, there is a large degree of lock-in . . . . [I]t is very unlikely that a company will go through the expense of uninstalling that system and switching to a different ERP system.").

347 *See* Charl van der Walt, *Assessing Internet Security Risk, Part 4: Custom Web Applications*, SYMANTEC, http://www.symantec.com/connect/articles/assessing-internet-security-risk-part-4-custom-web-applications (last updated Nov. 2, 2010) (discussing the variables considered when creating custom applications).

second custom software package, or to alter standard software to fit.[348] Similarly, organizations that use ERP software, such as SAP ERP, rely upon it as the core of their businesses—the application handles financial reporting, accounting, customer-relationship management, and other key tasks.[349] Duplicating ERP functionality increases costs by, for instance, sacrificing efficiency.[350] Organizations with custom applications or ERP software are likely to protest heterogeneity requirements with special fervor because they have incurred a substantial fixed cost that they will resist duplicating.

While ERP and custom applications are a nontrivial challenge for heterogeneity, several responses might mitigate the problem. First, for critical infrastructure, the federal government could defray part of the cost of diversifying over a period of years.[351] If firms with such applications agreed to migrate to a heterogeneous infrastructure—say, over five years—the government could offer either direct grants or tax incentives to reduce the firms' new technology and testing costs. The government operates similar programs to encourage change in other markets: for example, it will spend an estimated $7.5 billion to subsidize purchases of fuel-efficient vehicles from 2012 to 2019.[352] Moreover, cost relief seems appropriate in light of the positive externalities that greater cybersecurity creates.

Second, it may be possible to achieve partial heterogeneity. A firm that uses ERP software for finance, manufacturing, and customer-relations management may be able to move one function to a different platform more readily than it can migrate all three.[353] Finally, greater heterogeneity in underlying hardware and operating systems and greater disaggregation of information can compensate partially for a single, monolithic application.

As with increasing disaggregation, boosting IT heterogeneity comports with the tenets of normal accident theory. It reduces how tightly systems are coupled and may reduce interactivity.[354] As a result, systems may be less vulnerable to errors and can recover from such errors more quickly. Heterogeneity loosens

---

348 *See, e.g.*, ROE & SCHULMAN, *supra* note 92, at 160-63 (describing custom energy-grid-management software).

349 *ERP Solutions*, SAP, http://global.sap.com/solutions/business-suite/erp/featuresfunctions/operationalanalysis.epx (last visited Mar. 22, 2014).

350 *See* HUGOS & HULITZKY, *supra* note 346, at 94.

351 *See* Bambauer, *Conundrum*, *supra* note 26, at 651-53 (proposing government subsidies to supplement investment in diversifying data systems).

352 CONG. BUDGET OFFICE, EFFECTS OF FEDERAL TAX CREDITS FOR THE PURCHASE OF ELECTRIC VEHICLES, at iii (Sept. 2012), *available at* http://www.cbo.gov/sites/default/files/cbofiles/attachments/09-20-12-ElectricVehicles_0.pdf.

353 *See ERP Solutions*, *supra* note 349.

354 *See* PERROW, *supra* note 88, at 79, 93-94 (discussing the effect of interactivity on the control and management of a system).

coupling by introducing artificial breaks in the system.[355] For example, an organization that uses Windows 8 as its only operating system has tightly coupled its computers: a successful Windows-based exploit would deliver control over all of its PCs. But when that organization introduces Macs, it decreases the coupling and a Windows attack would affect only some of the firm's machines. Heterogeneity, therefore, acts as a firebreak.

Increasing diversity may also decrease interactivity, which measures the degree to which a change in one part of the system affects other parts.[356] Here, heterogeneity has dichotomous effects. Increasing the number of components likely increases the chance that components will interact.[357] However, it also decreases the size of the effect if that interaction occurs. The net effect depends on which aspect of the change—likelihood or magnitude—dominates.

Diversity is an investment. For instance, ecologists have shown that monoculture agriculture is highly efficient and effective: farmers who specialize in one crop can use the same fertilizer, pesticides, and harvesting techniques on all their land.[358] However, it is also vulnerable. In an ecosystem where pathogens evolve over time, a single successful attack (such as by parasites) can generate catastrophic failure.[359]

Similarly, sensible investors purchase diversified assets. Index funds may underperform compared to particular stocks in the short term, but over longer periods, their returns are more stable.[360] Investing in only a single vehicle is an all-or-nothing bet—a painful lesson many Enron employees learned.[361] Thus, while spending on diversity incurs short-run costs, organizations would be wise to hedge their bets against cybersecurity risks by doing so.

---

355 *See id.* at 332 ("Accidents will be avoided if the system is . . . loosely coupled . . . because loose coupling gives time, resources, and alternative paths to cope with the disturbance and limits its impact.")

356 *Id.* at 72-79.

357 *See id.* at 73-74 (providing an example in which introducing additional components to an independent subsystem led to an unexpected interaction with a separate, unrelated subsystem).

358 *See* Miguel A. Altieri, *Modern Agriculture: Ecological Impacts and the Possibilities for Truly Sustainable Farming*, AGROECOLOGY IN ACTION, http://nature.berkeley.edu/~miguel-alt/modern_agriculture.html (last visited Mar. 22, 2014) (explaining that monoculture agriculture is "rewarded by economies of scale" and that increases in such systems means that "the whole agricultural support infrastructure . . . has become more specialized").

359 *Id.* (noting that a huge area with a single crop is vulnerable to a new "pathogen or pest").

360 *See* Mark Hulbert, *The Index Funds Win Again*, N.Y. TIMES, Feb. 22, 2009, at BU5 (explaining the wisdom of investing in index funds).

361 *See 401(k) Investors Sue Enron*, CNNMONEY (Nov. 26, 2001), http://money.cnn.com/2001/11/26/401k/q_retire_enron_re (estimating that Enron employees lost a total of $850 million on stock held in their retirement accounts).

In short, heterogeneity in information technology systems helpfully reduces their vulnerability to a single, potentially catastrophic exploit.

D. *Driving "Divide and Differ"*

To facilitate the adoption of disaggregation and heterogeneity in the private sector, the federal government should employ a mixture of carrots and sticks. First, Congress should condition awards of government contracts upon an adequate showing of a firm's efforts to re-architect its computer systems to embody these two principles. Second, Congress should enact legislation targeting key industries that mandates gradual implementation of these principles. Since resistance is likely, such a mandate should include carrots in the form of subsidies or tax credits to offset part of the cost of the changes. These measures overlap to some degree: some firms regulated by the stick will also partake of the carrots. This overlap is helpful because it reduces perceived and actual burdens of compliance. And it is likely necessary, since passing regulatory mandates is nearly certain to take more time than passing spending bills with conditions attached. The following Sections describe both efforts.

E. *Carrot: Bribe*

The federal government should use bribes to lure firms to implement disaggregation and heterogeneity—to divide and differ. Federal contracts can create a substantial incentive. The federal government spends roughly 14% of its annual budget—over $500 billion—on purchases of private-sector goods and services.[362] Small businesses receive nearly one-quarter of that largesse.[363] Some large firms, such as defense contractors Lockheed Martin, SAIC, and Raytheon, depend upon government contracts for more than half of their annual revenues.[364] As a condition of eligibility for government contracts, firms should be required to certify, under penalty of perjury and disqualification from contracting for a period of years, that they have

362 Robert Brodsky, *Contracting Spending Dips for the First Time in 13 Years*, GOV'T EXECUTIVE (Feb. 3, 2011), http://www.govexec.com/oversight/2011/02/contracting-spending-dips-for-the-first-time-in-13-years/33238; Jeanne Sahadi, *Cutting Washington Could Hit Main Street*, CNNMONEY (July 23, 2012), http://money.cnn.com/2012/07/23/news/economy/federal-spending/index.htm.

363 Sahadi, *supra* note 362.

364 *See* Kim Bhasin, *15 Companies that Will Get Crushed When the Government Stops Spending*, BUS. INSIDER (June 3, 2011), http://www.businessinsider.com/top-federal-government-contractors-2011-5?op=1.

implemented these principles in their computing infrastructures.[365] Alternatively, if firms outsource IT functions, they should be required to certify that their contracts with those providers mandate implementing similar requirements, and to identify what steps they have taken to ascertain the providers' compliance. To give this requirement teeth, the government should condition the contract on the firm's documenting its compliance.[366] In addition, the government should have the ability, under the contract, to audit compliance; a finding of more than token noncompliance should disqualify the contractor from bidding on contracts for a number of years.[367] This "audit with bite" seeks to drive compliance through the power of the purse while avoiding the overhead costs incurred through more formal documentation of controls, as required under the Sarbanes–Oxley Act.

The federal government has contemplated using its purchasing power for security purposes before. During the encryption debates of the 1990s, the Clinton Administration issued a proposed specification for a cryptosystem that would have allowed the government to access escrowed encryption keys with a court order.[368] While the specification was not formally binding, the government sought to purchase only telecommunications equipment using this "Clipper Chip" system and sweetened the deal by exempting Clipper gear from export restrictions.[369] Though Clipper ultimately failed due to opposition based on concerns about privacy and civil liberties, its opponents initially feared its adoption because of the government's massive spending influence.[370]

Similarly, the federal government has used its spending capabilities to influence IT infrastructure. Section 508 of the Workforce Investment Act of 1998 mandates that federal agencies ensure their IT systems afford individuals

---

365 *Cf.* 15 U.S.C. § 7241(a) (2012) (requiring that certain corporations certify their compliance with internal controls).

366 *Cf. id.* § 7262 (requiring that certain corporations submit an annual internal-control report).

367 *See generally* Carol Dinkins & Sean Lonnquist, *The Belt and Suspenders Approach: The Advantages of a Formalized Environmental Compliance Program*, 2009 UTAH L. REV. 1129, 1143-45 (2009) (discussing the EPA's imposition of a general business ethics–compliance program for its government contractors, the violation of which could lead to debarment from future contracts).

368 *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 764-72 (1995) (discussing the doubtful legal authority of the Escrowed Encryption Proposal, an expansive administrative project to make substantive security policy).

369 *Id.* at 770-71 (demonstrating the practical effect of the program in coercing public compliance). The government also would have benefited from network effects: private firms and individuals would likely purchase telecommunications equipment that could interoperate with Clipper-enabled devices, further embedding the standard. *Id.*

370 *Id.* at 773-76; *see also* A. Michael Froomkin, *It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15, 32-33 (explaining the popular backlash to the executive's plan to use the government's power as a major consumer to influence the market).

with disabilities access to information comparable to that available to nondisabled individuals.[371] The requirement covered both the use and the procurement of systems.[372] Accordingly, vendors and government contractors moved quickly to ensure that their systems rendered information accessible to those with disabilities.[373] As software vendor Adobe put it, "[C]ompanies will no longer be able to sell federal agencies any software or hardware that fails to meet accessibility standards."[374]

And in 2008, Congress passed the Higher Education Opportunity Act (HEOA) as part of its economic stimulus package.[375] One set of HEOA provisions imposes requirements upon institutions of higher education.[376] For their students to be eligible for federal financial aid, schools must implement technological deterrents to unlawful file sharing. The legislation gives schools several options for compliance, but conditions indirect governmental funding on adjusting computer networks to reduce copyright infringement.[377] Schools have moved rapidly to comply.[378]

The federal government can use the lure of lucrative contracts to push private companies to voluntarily adopt the design principles of disaggregation and heterogeneity. This creates two issues. First, how much must companies divide and differ to be eligible? Congress should set equal requirements in both the contracting and the regulatory contexts, which would ease the overall regulatory burden as some regulated firms would already meet the new criteria. Thus, contracting eligibility should depend upon meeting the standards described below. Second, what should be done to augment cybersecurity in companies that are not government contractors, but whose systems are critical to national security? Section F addresses these questions.

---

371 29 U.S.C. § 794d (2006).

372 *Id.*

373 *See, e.g.*, *Accessibility Standards*, ADOBE, http://www.adobe.com/accessibility/508standards.html (last visited Mar. 22, 2014).

374 *Id.*

375 Pub. L. No. 110-315, 122 Stat. 3078 (2008) (codified as amended in scattered sections of 20 U.S.C.).

376 20 U.S.C. § 1094(a)(29) (2012).

377 H.R. REP. NO. 110-803, at 548 (2008) (Conf. Rep.).

378 Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 887-89 (2012) (describing the University of Dayton's efforts to use a technology deterrent to meet HEOA requirements and maintain federal financial aid eligibility).

F. *Stick: Regulation*

The federal government must require firms in key industries to address the known unknowns. It should mandate that companies in a few critical sectors—and all government entities—implement disaggregation and heterogeneity in their computer systems. It should set an aggressive deadline for compliance, and alleviate the burden with funding for re-architecture efforts. Congress should pass legislation setting statutory defaults for these principles while authorizing regulators to impose either more stringent or more lax requirements after notice-and-comment rulemaking. Finally, the new regime should permit affected private-sector entities to seek partial waivers if they can demonstrate either equal mitigation through other techniques or the need for greater time due to special circumstances. These regulatory measures are likely to be expensive and politically unpopular; however, they are also vital if America is serious about improving cybersecurity.

1. Defining the Regulated

The first question regarding regulation is scope: Who should be covered by the divide-and-differ requirements? To date, presidential and congressional cybersecurity proposals have sought expansive coverage, with the number of industries and firms constituting "critical infrastructure" metastasizing over time. For example, Homeland Security Presidential Directive 7 establishes a National Monuments and Icons Sector for critical infrastructure, which is overseen by the Department of the Interior.[379] Something has gone awry when the Grand Canyon is designated as critical infrastructure. Cybersecurity's ambit is thus ever-widening. To succeed—politically as well as technologically—cybersecurity legislation must be far more focused. This requires taking a hard look at what elements of industry are genuinely at risk and indispensable to national security.

Regulation should focus on six key sectors: finance and banking, defense contracting, transportation, utilities, government (federal, state, and local), and hospitals and medical centers. The importance of the financial sector is straightforward. Banks and financial firms have been targeted frequently for

379 *Homeland Security Presidential Directive 7: Directive on Critical Infrastructure Identification, Prioritization, and Protection*, 2 PUB. PAPERS 1739, 1741 (Dec. 17, 2003), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1739.pdf; *Understanding the National Monuments and Icons Sector*, DEP'T OF HOMELAND SECURITY http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/natMonument1.htm (last visited Mar. 22, 2014).

cyberattacks and espionage.[380] Defense contractor security directly implicates national security—these companies have been targeted repeatedly for espionage by China and other countries.[381]

Transportation is critical to America's economy. The economic effects of disruption can be extrapolated from case studies. For instance, when transit workers for New York City's subway system went on strike for three days in 2005, the city's economy lost an estimated $1 billion.[382] In 2002, the closure of twenty-nine West Coast ports for eleven days due to a labor dispute generated economic costs between $6 billion and $20 billion.[383] Even the collapse of a single interstate highway bridge in Minneapolis cost Minnesota $17 million in 2007 and $43 million in 2008 (until the bridge was replaced that year).[384]

Similarly, utilities are economically vital and pose a significant cybersecurity risk. They are often local monopolies and represent a single point of failure in key infrastructure such as power, water, waste treatment, and communications.[385] Further, utility operators increasingly attach their systems to networks that pass Internet traffic—often without sufficient precautions.[386]

---

380 *See, e.g.*, *Federal Reserve Hacked*, GUARDIAN (Feb. 6, 2013), http://www.guardian.co.uk/business/2013/feb/06/federal-reserve-anonymous (describing the attack by Anonymous that allegedly resulted in the theft of information of over 4000 bankers); Nicole Perlroth & Quentin Hardy, *Bank Hacks Were Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 9, 2013, at B1 (covering a denial-of-service attack against major banks); Michael Riley, *U.S. Spy Agency Is Said to Investigate Nasdaq Hacker Attack*, BLOOMBERG (Mar. 30, 2011), http://www.bloomberg.com/news/2011-03-30/u-s-spy-agency-said-to-focus-its-decrypting-skills-on-nasdaq-cyber-attack.html (describing the breach of Nasdaq computers).

381 *See China Under Suspicion in U.S. for Lockheed Hacking*, REUTERS (June 2, 2011), http://www.reuters.com/article/2011/06/02/us-lockheed-china-idUSTRE7517B120110602; Michael Riley & John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG (Dec. 14, 2011), http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html (discussing the tendency of Chinese cyberspies to attack U.S. companies).

382 *See* Chris Dolmetsch & Josh P. Hamilton, *Transit Workers Agree to End Strike; Talks Continue (Update11)*, BLOOMBERG (Dec. 22, 2005), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aFC2LP.c9cro&refer=us.

383 *See* Andrew Leonard, *The Costs of a Port Shutdown*, SALON (Dec. 13, 2011), http://www.salon.com/2011/12/13/the_costs_of_a_port_shutdown.

384 *Economic Impacts of the I-35W Bridge Collapse*, POSITIVELY MINN. (Minn. Dep't of Transp., St. Paul, Minn.), *available at* http://www.dot.state.mn.us/i35wbridge/rebuild/municipal-consent/economic-impact.pdf.

385 *See, e.g.*, *Cuomo: Utilities Have Failed in Aftermath of Sandy; Suggests They Could Lose Monopolies*, CBS NEW YORK (Nov. 5, 2012), http://newyork.cbslocal.com/2012/11/05/cuomo-says-utilities-failed-during-sandy-suggests-they-could-lose-monopolies (demonstrating the ramifications of disruptors to single companies that hold a monopoly over utilities); Lakis Polycarpou, *What Is the Benefit of Privatizing Water?*, COLUMBIA U. EARTH INST. (Sept. 2, 2010), http://blogs.ei.columbia.edu/2010/09/02/what-is-the-benefit-of-privatizing-water (noting the benefits and drawbacks of the trend of municipalities to privatize utility supply in local monopolies).

386 *See* James R. Koelsch, *Web-Based SCADA Gathers More Fans*, AUTOMATION WORLD (Dec. 5, 2012), http://www.automationworld.com/control/web-based-scada-gathers-more-fans (describing how

Governments both hold sensitive information and deliver vital services such as law enforcement, emergency services, and national defense.[387] Moreover, holding governments to the same cybersecurity requirements as the private sector should help ensure that burdens are manageable and that government entities do not become a threat to more secure private entities.

Lastly, hospitals and medical centers maintain highly sensitive information and provide critical services. They, too, have been increasingly targeted by hackers.[388] These six core economic sectors present the highest-value targets for cyberattacks and are vital to both society and U.S. national security. Accordingly, regulation mandating disaggregation and heterogeneity should concentrate on them.

2. Sticky Defaults

The most difficult question is this: What default requirements should Congress establish for disaggregation and heterogeneity? Legislation should set somewhat stringent defaults for two reasons. First, the notice-and-comment process described below can alter these settings if regulators are convinced that the cost–benefit calculus is incorrect. But setting stronger security mandates initially has a helpful anchoring effect.[389] Second, strong defaults usefully address information asymmetry. Regulators do not have access to private information held by regulated entities that could make their rules more effective and efficient.[390] This occurs because of both costs

---

accelerating implementation of "Web-based networks [for utility companies] increase[s] the risk of tampering by unauthorized people"); Paul Roberts, *Homeland Security Warns SCADA Operators of Internet-Facing Systems*, THREATPOST (Dec. 12, 2011), http://threatpost.com/homeland-security-warns-scada-operators-internet-facing-systems-121211/75990 ("[I]ndustrial control systems are given access to the Internet[, and] . . . critical infrastructure operators frequently fail to secure such systems . . . .").

387 *See generally* EXEC. OFFICE OF THE PRESIDENT OF THE U.S., THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, *available at* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (highlighting the initiatives established by the security council to help secure the U.S. government and its role in carrying out public services in cyberspace).

388 *See* Robert O'Harrow, Jr., *Health Systems at Risk of Hacking*, WASH. POST, Dec. 26, 2012, at A1; Neal Ungerleider, *Medical Cybercrime: The Next Frontier*, FAST COMPANY (Aug. 15, 2012), http://www.fastcompany.com/3000470/medical-cybercrime-next-frontier (noting the trend of cyber-attacks on hospitals to steal or damage medical records).

389 *See* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science, and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 602 (2006) (explaining the cognitive bias toward "status quo" settings).

390 *See* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 678 (2010) ("Regulators, moreover, lack a clear vantage point for identifying . . . private information about firm organization necessary for developing top-down requirements of risk-mitigating behavior.").

and strategic behavior. It is expensive for regulators to gather information, even when it is offered willingly by firms.[391] In addition, firms may be unwilling to share since inexact information may let them evade the rules.[392] However, unattractive defaults can force their hands. This method parallels Ian Ayres and Robert Gertner's approach to contract doctrine.[393] They suggest setting default contract rules to force the revelation of private information; by making those defaults sufficiently unattractive, parties will bargain around them.[394] Penalty defaults can work equally well for cybersecurity.

Statutory defaults should address data stores for disaggregation and hardware and software for heterogeneity. For disaggregation, legislation should impose a rule of halves: a breach of any given data center or data warehouse should expose no more than half of an entity's data to unauthorized access or alteration. This mandate should be manageable for organizations since mirrored data centers are standard practice for corporations.[395] However, this requirement could create significant additional costs. A firm seeking to mirror its data warehouse would need to move from two data centers at present to four under this requirement, since each location would house half the entity's information. But organizations can mitigate these costs by introducing separation (such as via isolated networks and buildings) into their IT systems—in effect, subdividing a single data center into multiple units. Regulation should thus require entities to, at minimum, bifurcate their data stores.

For heterogeneity, legislation should impose a rule of thirds: at least one-third of covered hardware and software must be from a different vendor than the other two-thirds. Covered hardware should include servers, workstations, and network hardware. Covered software should include operating systems and applications (including antivirus programs, firewalls, and intrusion-detection systems).[396]

---

391 Tom C.W. Lin, *A Behavioral Framework for Securities Risk*, 34 SEATTLE U. L. REV. 325, 366-67 (2011) (describing resource constraints that prevent the SEC from effectively monitoring securities risk factors).

392 Steven L. Schwarcz, *Rethinking the Disclosure Paradigm in a World of Complexity*, 2004 U. ILL. L. REV. 1, 22-23 (noting parties' incentives to structure transactions to avoid regulation).

393 *See generally* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87 (1989). I thank Endre Stavang for this insight.

394 *Id.* at 96-100.

395 *See* Bambauer, *Conundrum*, *supra* note 26, at 645-46 (providing examples of data security practices that allow businesses to quickly return to normal operations after a breach).

396 I do not include network protocols in the heterogeneity requirement. While it would be valuable to use multiple protocols, the near-ubiquity of TCP/IP makes implementing such a rule extremely difficult and costly. *See id.* at 598-601.

The hardware requirement should be comparatively easy for firms to meet, since there is already robust competition in the relevant markets—a company running IBM Blade servers can readily purchase HP Proliant ones. Firms will sacrifice some purchasing power through decreased volume, at least slightly increasing costs. The software requirement, however, is more difficult. Microsoft dominates workstation operating systems with Windows, and office productivity software with Office.[397] Moreover, as described above, organizations running ERP software or custom applications could incur significant costs when adding another option.

For some niches, though, there are readily available (and sometimes low-cost) alternatives. Companies can use workstations running Apple's Mac OS, or a Linux variant (which is free to acquire).[398] They can install OpenOffice (another open-source program) for word processing or spreadsheet work. Nevertheless, the rule of thirds recognizes the software bind. It seeks to leave firms with a sizeable minority of functional or uncompromised systems if an attacker exploits a vulnerability in the majority operating system or application. And it further tries to minimize the market effects of a rule that would, in effect, drive purchases away from dominant vendors such as Microsoft.[399] Such a rule of thirds is manifestly imperfect, but it is workable.

3. Due Dates

Firms should be given an aggressive deadline for implementing divide and differ. A useful analogy is the effort to address the Year 2000—or Y2K—problem in the last years of the twentieth century. The Y2K problem resulted from a programming shortcut intended to conserve memory: software and hardware frequently stored the year portion of a date as a two-digit number, so 1999 would be represented as "99."[400]

Policymakers slowly realized the uncertainty inherent in the change to a new century.[401] No one could reliably predict how software would handle

---

397 Rosenblatt, *supra* note 339 (illustrating Windows' market-share dominance); *see also* Trefis Team, *An Overview Why Microsoft's Worth $42*, FORBES (Jan. 9, 2013), http://www.forbes.com/sites/greatspeculations/2013/01/09/an-overview-why-microsofts-worth-42 (documenting Office's 95% market share).

398 *See* RAYMOND, *supra* note 68, at 19-25.

399 *See* Bambauer, *Rules, Standards, and Geeks*, *supra* note 143, at 53 (noting the risk of market-making effects if one technology is selected for regulatory compliance).

400 *See* Farhad Manjoo, *Apocalypse Then*, SLATE (Nov. 11, 2009), http://www.slate.com/articles/technology/technology/features/2009/apocalypse_then/was_y2k_a_waste.html.

401 John Quiggin, *The Y2K Scare: Causes, Costs and Cures*, AUSTL. J. PUB. ADMIN., Sept. 2005, at 46, 48-49 (describing government programs adopted to mitigate IT failures due to Y2K).

date calculations. A massive remediation effort was launched, involving testing, updating, and verifying nearly every extant piece of hardware and software.[402] Nearly all of that effort occurred in less than two years' time, during 1998 and 1999.[403] The cost of Y2K remediation during those two years was enormous—estimated at $500 billion worldwide and $100 billion in the United States.[404] Some of those costs could have been reduced had organizations begun remediation earlier. Yet, Y2K is proof that firms can successfully undertake large-scale IT restructuring in a relatively short period of time.[405]

One factor that should be included in setting a deadline is the typical life cycle of computer systems. A roughly three-year depreciation cycle is common: on average, hardware is replaced every three to four years.[406] This means that companies can, by shifting their procurement strategies, achieve significant heterogeneity quickly—they replace an average of 25% to 33% of their computers each year. The heterogeneity requirement mandates that at least 33% of an entity's computers be from a different vendor than the others. An organization could achieve this goal in about a year if it purchased its replacement machines from a different manufacturer. In combination with the Y2K case study, this suggests that a three-year deadline for compliance with the disaggregation and heterogeneity requirements is practicable—challenging, but manageable.

4. Another Bribe

The government should lessen the burden of implementing divide and differ with generous funding. While increased spending is politically difficult in a time of economic downturn and rising expenditures on entitlement programs, better cybersecurity is a vital matter of national security. Break-ins at defense contractors, cyberattacks on the Federal Reserve, and

---

402 *Id.* at 47.

403 *Id.* at 49.

404 U.S. SENATE SPECIAL COMM. ON THE YEAR 2000 TECH. PROBLEM, Y2K AFTERMATH—CRISIS AVERTED: FINAL COMMITTEE REPORT 11-12 (Feb. 29, 2000), *available at* http://permanent.access.gpo.gov/lps90964/y2kfinalreport.pdf.

405 Manjoo, *supra* note 400 ("[W]ithin just a couple years, small and large companies were able to review completely and fix computer code that had been kicking around in their systems for decades.").

406 *See, e.g.*, TIMOTHY MOREY & ROOPA NAMBIAR, INTEL CORP., USING TOTAL COST OF OWNERSHIP TO DETERMINE OPTIMAL PC REFRESH CYCLES 11-12 (updated Jan. 2010), *available at* http://www.intel.com/content/dam/doc/white-paper/pc-upgrade-industry-study-using-total-cost-of-ownership-to-determine-optimal-pc-refresh-lifecycles-paper.pdf; Leslie Meredith, *How Often Should Company Computers Be Replaced?*, BUS. NEWS DAILY (July 18, 2010), http://www.businessnewsdaily.com/65-when-to-replace-the-company-computers.html.

hacks of critical infrastructure make plain the character of the risk.[407] Spending on disaggregation and heterogeneity is an investment, not only against cyberattacks and espionage, but also against more mundane threats, such as natural disasters.

Specifying the level of funding that the federal government should dedicate to the problem is likely impossible, as it depends upon too many contingent factors. Instead, the government should concentrate on several core objectives. First, legislation should be attentive to easing demands on smaller entities.[408] The burdens of added cost and technological complexity may be particularly acute for small businesses. Nearly 40% of reported cyberattacks in the first part of 2012 targeted businesses with fewer than 500 employees, yet in a survey of small businesses conducted in September 2012, "60% of respondents admitted they have no plan" to deal with data breaches, and "66% said they are not concerned about cyber threats."[409] The federal government has a history that should be continued of easing burdens for small firms.[410]

Second, the funding should be transitional—it should ease the cost of moving to a disaggregated data environment that runs on heterogeneous components. Once organizations have undertaken the necessary structural changes, they should support the ongoing costs of this new environment. In the Broadband Technology Opportunity Program, for example, the federal government funded the costs of building additional network capacity but left the ongoing operational costs to the companies operating those networks.[411] In the short run, though, the government should underwrite a share of the overhead costs for the changeover, perhaps with a bonus for early movers via a phaseout in subsidies. To keep recordkeeping burdens manageable, the legislation could structure financial support as a refundable tax credit. Such a credit would both provide supporting documentation for a firm's expenses through the standard reporting process and ensure that even

---

407 *See supra* notes 380-86 and accompanying text.

408 *Cf.* Frances Robinson, *EU to Set Out Proposals for New Rules on Cybersecurity–Draft*, WALL ST. J. (Feb. 4, 2013), http://online.wsj.com/article/BT-CO-20130204-708228.html (exempting "micro enterprises" from sanctions for failure to comply with new cybersecurity rules "to avoid an excessive administrative burden on small businesses").

409 John Fontana, *On Cybersecurity, Small Businesses Flirting with Disaster, Survey Finds*, ZDNET (Oct. 17, 2012), http://www.zdnet.com/on-cybersecurity-small-businesses-flirting-with-disaster-survey-finds-7000005891.

410 Bambauer, *Conundrum*, *supra* note 26, at 651-52.

411 Notice of Funds Availability, Broadband Technology Opportunities Program (BTOP), 75 Fed. Reg. 3792, 3794-95 (Jan. 22, 2010) (listing requirements for BTOP funding).

firms without net tax liability would benefit, since they could obtain refunds where eligible.[412]

Lastly, the government should not cap total expenditures on cybersecurity funding, since the program is a form of social insurance against cybersecurity risks. The government already spends significant funds on similar insurance. In 2012 alone, the government spent $1 billion on food safety and inspection,[413] up to $7 billion on flood insurance claims (along with hundreds of millions of dollars in interest payments on loans),[414] and $3.2 billion in crop insurance.[415] A one-off investment in cybersecurity may be costly initially, but it will pay dividends in reduced risk in the long term. This can be fiscally sensible: consider, for example, that the federal government spent approximately $150 million on flood mitigation efforts in 2013, thereby avoiding roughly $1.7 billion in flood-related losses.[416] The government should spend now to save later.

5. Bespoke Regulation

The legislation that implements divide and differ should tailor its requirements to permit regulators to alter terms after notice-and-comment rulemaking. The statutory mandates for disaggregation and heterogeneity should act as defaults, but since they are likely to be crude ones, Congress should empower regulators to make more refined demands.[417] The rulemaking should fall upon the federal agency or agencies already responsible for the particular sector. For some economic sectors, the relevant regulator is straightforward: for example, requirements for utilities should be set by the Department of Energy (probably by the Federal Energy Regulatory

---

412 Ruth Mason, *Federalism and the Taxing Power*, 99 CALIF. L. REV. 975, 1015-16 (2011) (discussing advantages of refundable tax credits); *cf.* U.S. DEP'T OF THE TREASURY, THE AMERICAN OPPORTUNITY TAX CREDIT 4-6 (Oct. 12, 2010), http://www.treasury.gov/resource-center/tax-policy/Documents/American-Opportunity-Tax-Credit-10-12-2010.pdf (describing the American Opportunity Tax Credit's advantages over previous nonrefundable tax credits).

413 U.S. DEP'T OF AGRIC., FY 2012: BUDGET SUMMARY AND ANNUAL PERFORMANCE PLAN 66 (2012), http://www.obpa.usda.gov/budsum/FY12budsum.pdf.

414 Eric Lipton, Felicity Barringer & Mary Williams Walsh, *Flood Insurance, Already Fragile, Faces New Stress*, N.Y. TIMES, Nov. 13, 2012, at A1.

415 U.S. DEP'T OF AGRIC., *supra* note 413, at 4.

416 DEP'T OF HOMELAND SEC., FED. EMERGENCY MGMT. AGENCY, NAT'L FLOOD INS. FUND, FISCAL YEAR 2013: CONGRESSIONAL JUSTIFICATION, at 1-2, 9-10 (2013), *available at* http://www.fema.gov/pdf/about/budget/11h_fema_nfi_fund_dhs_fy13_cj.pdf.

417 *Cf.* David A. Super, *Against Flexibility*, 96 CORNELL L. REV. 1375, 1407-08 (2011) ("The law often relies on default rules to respond to shortages of information, normative guidance, or decisional capacity . . . . These . . . effectively serve as lower-quality substitutes for the desired inputs." (footnotes omitted)).

Commission).[418] By contrast, for the financial sector, there is a congeries of regulators, including various elements of the Department of the Treasury, the Federal Reserve, and the Federal Deposit Insurance Corporation.[419] As with the GLBA's security requirements discussed above, these regulators should coordinate to issue joint regulations.

The more refined requirements are designed to achieve appropriate levels of disaggregation and heterogeneity at the lowest cost.[420] The legislation should preclude firms from seeking to substitute prevention measures for mitigation ones and from emphasizing their precautions. Rather, regulators should consider how regulated entities may best achieve resilience.[421] For example, firms in a particular subsector might hold only nonsensitive information and be able to recover from cyberattacks quickly due to advanced backup and recovery techniques. In that case—where espionage is unlikely and hacking can be rapidly addressed by recovery—regulators might impose less stringent requirements for data separation and variegated components.

One virtue of the rulemaking process is that it will force regulated entities to engage with the underlying goals of the statute. Firms fighting about "divide and differ" will have to take stock of how their computer systems score on these criteria. And, the notice-and-comment period may cause organizations to reveal information about best practices or other steps they take to improve resilience and mitigate the effects of attacks or spying.

6. Respite

Lastly, Congress should allow regulated entities to seek waivers from the divide-and-differ requirements if they can prove equally effective at mitigating risk through other techniques or if they can demonstrate a pressing need for more time to comply. For the former, the implementing legislation should incorporate flexibility. In unusual cases, it could permit firms to trade off among the two goals. For instance, a company forced to rely on a single, customized application might increase disaggregation of its information and networks, such as physically separating networks or disconnecting

---

418 *See What FERC Does*, FED. ENERGY REG. COMMISSION (Jan. 20, 2014), http://www.ferc.gov/about/ferc-does.asp.

419 *See supra* note 271 (listing the agencies responsible for various financial regulations).

420 *Cf.* Gregg P. Macey, *Coasean Blind Spots: Charting the Incomplete Institutionalism*, 98 GEO. L.J. 863, 910-11 (2010) (suggesting that the cost of regulation should be a consideration in developing new regulations).

421 *Cf.* Burstein, *supra* note 299, at 181-82 & n.78 (noting that "'grateful degradation' of a network is central to the concept of resilience," and further "defining resilience as 'maintain[ing] a certain level of availability of performance even in the face of active attacks'" (alteration in original) (citation omitted)).

networks from the Internet.[422] The intent is to enable individual firms to achieve legislative goals at the lowest cost.

Similarly, if firms show a compelling need for more time to achieve disaggregation and heterogeneity, regulators should permit a short extension of the deadline—perhaps by twelve or eighteen months. Ultimately, time to comply is a proxy for cost. Thus, waivers should be considered where the statutory deadline imposes costs that threaten firms' economic viability or require diverting resources urgently needed for other issues (e.g., public safety improvements). Waivers should be unusual—the exception, rather than the rule. The deadline for divide and differ may be crude, but crude measures often suffice. And regulators should generally consider waivers on a wider basis than the individual firm—for example, offering them to all electrical utilities in rural areas, rather than a single such utility. If one firm deserves nonstandard treatment, its competitors likely do as well.[423] This approach should reduce strategic behavior and avoid rewarding organizations that have less effective infrastructure or personnel, while penalizing their more effective competitors.

7. The Net Effect

The combination of carrots and sticks should push firms in critical sectors to mitigate the effects of cyberattacks and espionage by quickly implementing the disaggregation and heterogeneity principles.

G. *Objections*

Three objections to the proposed regulatory model—the chosen mechanism, technological timidity, and its cost—deserve analysis. First, why employ top-down specifications rather than alternatives such as best practices or negligence standards? Second, why is the technological timidity evinced by regulators not fatal to the proposal? Third, would this system impose unsupportable costs on firms? This Article next addresses each objection.

The top-down regulatory model provides better notice to regulated entities than the alternatives, ensures national uniformity, and solves difficult

---

422 *See* Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 180-81 (2009) (noting the separation of networks as a cybersecurity defensive technique).

423 *Cf.* Bethany R. Berger, *What Owners Want and Governments Do: Evidence from the Oregon Experiment*, 78 FORDHAM L. REV. 1281, 1283-84 (2009) (discussing voter repeal of Oregon property regulation, which provided for waivers in some cases but not others).

information problems. First, alternatives such as negligence[424] or best-practices[425] standards provide firms notice about requirements only gradually and retrospectively. Technology changes rapidly. Adjudication is always retrospective and always slow: it tells organizations what the proper level of security was at the time the harm occurred, but not now. Negligence also uses a negative-notice model: it tells firms what precautions are inadequate, but not necessarily which are sufficient. Finally, negligence-focused analyses frequently falter in assessing harm and causation. Under this standard, insecure data controllers rarely face liability.[426] Courts either find a lack of actionable harm, or a failure to link harm that occurs to insecure handling of information.[427] These hurdles are both conceptually and practically problematic. They suggest that a negligence standard would not effectively boost security.

Similarly, best practices take time to disseminate and run the risk (familiar from tort law) that an entire industry may take insufficient precautions.[428] Insecurity appears to be widespread—even sophisticated entities suffer successful attacks. These risks are exacerbated by cybersecurity's externalities and information asymmetries. Best practices, too, respond to the diffuse threat of legal liability. Consumers have difficulty detecting laggards, and firms do not bear the full cost of insecurity.

Moreover, a common law–negligence approach, as used in tort law, risks the imposition of different standards in different jurisdictions. But cybersecurity is a national problem: attackers do not care whether a firm is based in Biloxi or Boston.[429] Indeed, varying standards could invite attacks against

---

424 *See* Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113, 155 (2011) (noting that negligence could be used in creating remedies to cybersecurity breaches).

425 *See* Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1210 n.101 (2011) (discussing the limits of private best-practice agreements because such practices would apply only to those who agree to follow them).

426 *See* Bambauer, *Rules, Standards, and Geeks*, *supra* note 143, at 58 (arguing that courts largely exempt data owners from tort liability).

427 *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding that the plaintiffs had alleged only hypothetical injury and thus had no standing to file suit against the corporation when the plaintiffs' personal information was exposed in a data breach); Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1078-79 (2009) (explaining the legal hurdles that plaintiffs face in personal-data privacy actions).

428 *See The T.J. Hooper*, 60 F.2d 737, 738 (2d Cir. 1932) (finding tugboat companies liable for failing to employ radios to monitor weather forecasts, even though radios were not standard in the industry).

429 *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, CYBERSECURITY: NATIONAL STRATEGY, ROLES, AND RESPONSIBILITIES NEED TO BE BETTER DEFINED AND MORE EFFECTIVELY IMPLEMENTED (2013), *available at* http://www.gao.gov/assets/660/652170.pdf (examining the national dimension of cybersecurity risks).

entities in relatively low-security states or locations.[430] Therefore, cybersecurity requires a uniform national standard.

Lastly, best practices and negligence evolve over time. Normally, this flexibility is a strength; however, for cybersecurity, it is a weakness: successful attacks must occur to develop a standard, and refinement of that standard can occur only with subsequent breaches or hacks. Harm drives information development: regulators, including courts, learn only when cyberattacks cause harm. But, the harm still occurs.[431] The cost of harm is increasingly high and outweighs whatever benefits accrue from using a standard rather than a rule to assess disaggregation and heterogeneity.

The divide-and-differ system is designed to address regulators' technological timidity. The requirements are design principles, not specific features or capabilities. As such, regulators need little, if any, expertise to draft rules or evaluate compliance. They need not grapple with the relative merits of Linux, FreeBSD, or Windows operating systems. They must only verify that an organization employs more than one such system. Similarly, they do not have to understand the details of cloud computing; understanding that no single data store contains all of an entity's information is sufficient. These principles are likely to endure because they describe information architecture rather than specific products or technologies.[432] They are flexible: firms can implement a variety of mechanisms to meet the mandates. And they are clear—there is little uncertainty in how to fulfill disaggregation and heterogeneity goals. Divide and differ is cybersecurity regulation with training wheels.

This Article's regulatory proposal is also undeniably expensive, but those costs are both justified and partially offset. First, cybersecurity has been a top policy priority for at least fifteen years.[433] President Obama even took the unusual step of writing an opinion piece on cybersecurity for the *Wall Street Journal* in which he described cyberattacks as "one of the most serious economic and national security challenges we face."[434] In his 2013 State of

---

430 *Cf.* J. McIntyre Mach. v. Nicastro, 131 S. Ct. 2780, 2794 (2011) (Breyer, J., concurring) (noting variance in plaintiff success rates in tort cases and the risks for manufacturers that result from forum-shopping).

431 *Cf.* Gorman et al., *supra* note 303 (reporting a cybersecurity breach at the Defense Department's fighter jet project).

432 *See* Bambauer, *Rules, Standards, and Geeks*, *supra* note 143, at 52 (advocating for the use of general standards instead of specific rules when regulating most information technology, because technology develops rapidly).

433 *See* Bambauer, *Conundrum*, *supra* note 26, at 592 (noting cybersecurity proposals during the Clinton Administration).

434 President Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012), http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

the Union address, he again argued, "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[435] The director of the NSA estimated that cybercrime costs $1 trillion per year, constituting "the greatest transfer of wealth in history."[436] Further, a new National Security Estimate identifies cyberespionage as a major threat to the United States' economic competitiveness.[437] And former Secretary of Defense Leon Panetta has raised the frightening prospect of a "cyber 9/11."[438] This significant threat justifies significant expense. Since the 9/11 attacks, for example, federal government spending has risen by $110 billion on terrorist-related intelligence expenditures, in addition to the $200 billion increase in local government and private-firm spending.[439]

Second, insecurity creates a negative externality. Insecure organizations pass costs to others, even if only in the form of risk, without being penalized for them. This Article's proposal would cause insecure organizations to spend to upgrade security, which would force them at least partly to internalize these costs from risk.[440] Though the amount spent is unlikely to match precisely the amount of the externality, the regulatory mandate is similar in effect to a Pigouvian tax.[441] The mandate's costs are a crude means of mitigating the externality.

Third, the proposal contemplates having the federal government defray some of the mandate's costs. Since cybersecurity is a public good, subsidizing it from the public fisc is sensible. The lure of funding will likely reduce (though not eliminate) opposition to the legislation and will likely lessen its influence on firms' budget allocations.[442]

---

435 *Remarks by the President in the State of the Union Address*, WHITE HOUSE (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

436 *See* Peter Maass & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

437 Ellen Nakashima, *Cyber-Spying Said to Target U.S. Business*, WASH. POST, Feb. 11, 2013, at A1.

438 *See* David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES, Feb. 4, 2013, at A1 (describing a cyberattack scenario that would require military involvement).

439 John Mueller & Mark G. Stewart, *Does the United States Spend Too Much on Homeland Security?*, SLATE (Sept. 7, 2011), http://www.slate.com/articles/news_and_politics/politics/2011/09/does_the_united_states_spend_too_much_on_homeland_security.html.

440 Camp & Wolfram, *supra* note 136, at 18-19.

441 *See* A. Mitchell Polinsky & Steven Shavell, *Pigouvian Taxation with Administrative Costs*, 19 J. PUB. ECON. 385, 385-86 (1982) (defining a Pigouvian tax and explaining the costs associated with its use).

442 *Cf.* Ronald Brownstein, *Why the GOP's Resistance to Medicaid Expansion Is Eroding*, NAT'L J. (Feb. 7, 2013), http://www.nationaljournal.com/columns/political-connections/why-the-gop-s-resistance-to-medicaid-expansion-is-eroding-20130207 (describing how generous federal funding is leading states to expand Medicaid health insurance programs, even though doing so requires state expenditures).

Better cybersecurity is a sensible investment to combat a problem defined by America's leaders as grave. Firms can feel at least partly reassured that their government will help fund the divide-and-differ mandate and should realize—perhaps grudgingly—that some of its burden is warranted to offset externalities.

Thus, to guard against unauthorized access and alteration of information, cybersecurity law should mandate disaggregated, heterogeneous storage of information for entities in key economic sectors and for firms seeking government contracts.

IV. THE UNKNOWN UNKNOWNS

A. *The Threat*

Someone picked the locksmith's door.

The attack began via "Spear Phishing," a strategy where the attacker targets a specific set of users through a fraudulent email.[443] A number of employees at the security company RSA received email messages with the subject line "2011 Recruitment Plan."[444] Attached to the messages was a Microsoft Excel file containing an Adobe Flash movie.[445] When one employee opened the file, it launched the movie, which contained code that exploited a previously unknown bug in Flash.[446] Such zero-day attacks cannot be prevented technologically; defenders have no knowledge of the vulnerability that the attack exploits, and hence cannot defeat it.[447] A zero-day vulnerability is an unknown unknown: defenders are unaware of either its existence or its character.

The consequences for RSA were painful. The file installed a Remote Access Tool (RAT) giving the attacker control over the employee's computer.[448] The attacker monitored the computer and RSA's network, stealing user

---

443 Uri Rivner, *Anatomy of an Attack*, RSA (Apr. 1, 2011), https://blogs.rsa.com/anatomy-of-an-attack.

444 Elinor Mills, *Attack on RSA Used Zero-Day Flash Exploit in Excel*, CNET (Apr. 5, 2011), http://news.cnet.com/8301-27080_3-20051071-245.html.

445 Peter Bright, *Spearphishing + Zero-Day: RSA Hack Not "Extremely Sophisticated,"* ARS TECHNICA (Apr. 4, 2011), http://arstechnica.com/security/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated.

446 *Id.*

447 *See* O'Harrow, *supra* note 230 (defining a zero-day as "a vulnerability in the software that has never been made public and for which there is no known fix").

448 *See* Riva Richmond, *The RSA Hack: How They Did It*, N.Y. TIMES (Apr. 2, 2011), http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it (mentioning the "stealthy tool" that allows hackers to control a machine from afar); Rivner, *supra* note 443 (describing the Poison Ivy tool as an Advanced Persistent Threat).

credentials (login names and passwords) that allowed access to sensitive information about the SecurID tokens.[449] Though RSA detected the attack quickly, the damage was done: the company's parent firm, EMC, spent $66 million to help customers mitigate the damage.[450]

RSA's chairman stated that the compromised information "could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack."[451] He was right. Defense contractor L-3 Communications was hacked by attackers who used falsified codes from a SecurID token that was cloned using the stolen information from the RSA attack.[452] Around the same time, two other defense contractors reportedly suffered similar attacks.[453] This combination of human and computing weakness—of one gullible employee and one unknown vulnerability—led directly to national security harm to the United States.

A zero-day attack is akin to the Crane Kick in the movie *The Karate Kid*: if it is done properly, no defense is possible.[454] Zero-days have been at the heart of successful attacks on Iran's nuclear refinement facilities, Google's data stores, and American defense contractors.[455] This potency makes zero-days challenging for cybersecurity regulation. Formally, a zero-day attack is a weaponized exploit of a significant security flaw—an exploit

---

449 *Id.*; *see also* Bright, *supra* note 445 (explaining that access to SecurID converts a two-factor system into a single-factor, password-only system).

450 *See* Hayley Tsukayama, *Cyber Attack on RSA Cost EMC $66 Million*, WASH. POST (July 26, 2011), http://www.washingtonpost.com/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html ("[EMC] incurred an accrued cost associated with investigating the attack, hardening our systems and working with customers to implement our remediation programs.").

451 Letter from Art Coviello, Exec. Chairman, RSA, to RSA Customers (June 6, 2011), *available at* http://www.ncanet.com/resources/press-releases/91-2011-06-08-art-coviello-rsa-open-letter-customers.html.

452 *See* Fahmida Y. Rashid, *Northrop Grumman, L-3 Communications Hacked via Cloned RSA SecurID Tokens*, EWEEK (June 2, 2011), http://www.eweek.com/c/a/Security/Northrop-Grumman-L3-Communications-Hacked-via-Cloned-RSA-SecurID-Tokens-841662 (providing an overview of L-3 Communications and information about the attack).

453 *Id.*

454 THE KARATE KID (Columbia Pictures Corp. 1984). *But see The Karate Kid Crane Kick—No Can Defense?*, IKIGAIWAY (Feb. 6, 2012), http://www.ikigaiway.com/2012/the-karate-kid-crane-kick-no-can-defense (speculating that the crane kick may, in fact, be defensible).

455 *See* Fahmida Y. Rashid, *Adobe Zero-Day Exploit Targeted Defense Contractors*, EWEEK (Dec. 7, 2011), http://www.eweek.com/c/a/Security/Adobe-ZeroDay-Exploit-Targeted-Defense-Contractors-383203 (discussing attacks exploiting a vulnerability in Adobe Reader); Sanger, *supra* note 15 (discussing President Obama's secret orders to attack the computer systems running Iran's main nuclear refinement facilities); Zetter, *supra* note 170 (discussing the zero-day attacks on Google).

that neither software vendors nor antivirus firms know about.[456] Users targeted by the exploit are almost completely vulnerable to it: unless they can block the traffic implementing the attack—meaning they must detect such traffic—their systems will be compromised.[457]

Zero-day exploits are the most dangerous weapons in an attacker's arsenal, and security researchers have argued that commerce in such tools should be banned.[458] They help explain why cybersecurity is partial at best: certain aspects of the security problem cannot be solved. If Chinese security services discover a zero-day attack on Microsoft Windows, Windows users are vulnerable to that cyberweapon until it is independently discovered, accidentally patched, or voluntarily shared by China.[459]

Zero-days also present a disturbing dual trend: regulation of their use is effectively impossible, and a growing commercial market exists for their production, aggregation, and distribution.[460] While countries may be able to constrain their own use of exploits, they cannot effectively limit use by other nation-states. Zero-day attacks blur the line between espionage and war-like spying, they are difficult to detect and attribute to a particular source, and like war, they can damage their targets (and perhaps bystanders).[461] Combat can

---

456 *See* Brian Krebs, *Advanced Persistent Tweets: Zero-Day in 140 Characters*, KREBS ON SECURITY (May 3, 2011), http://krebsonsecurity.com/2011/05/advanced-persistent-tweets-zero-day-in-140-characters (analogizing zero-day attacks to ninjas due to their strength and anonymity); O'Harrow, *supra* note 220.

457 *See, e.g.*, TIPPING POINT, THE TOP CYBER SECURITY RISKS 21 (2009), *available at* http://www.dunkel.de/pdf/200909_TopCyberSecurityRisks.pdf (noting that when "a working exploit of the vulnerability has been released into the wild, users of the affected software will continue to be compromised until a software patch is available or some form of mitigation is taken by the user").

458 Ryan Naraine, *"0-day Exploit Middlemen Are Cowboys, Ticking Bomb*," ZDNET (Feb. 16, 2012), http://www.zdnet.com/blog/security/0-day-exploit-middlemen-are-cowboys-ticking-bomb/10294 (warning against the danger of trading vulnerabilities); Tom Simonite, *Welcome to the Malware-Industrial Complex*, MIT TECH. REV. (Feb. 13, 2013), http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex (explaining that the market for zero-days remains unregulated).

459 *See, e.g.*, Gregg Keizer, *Elite Hacker Gang Has Unlimited Supply of Zero-Day Bugs*, COMPUTERWORLD (Sept. 7, 2012), http://www.computerworld.com/s/article/9231051/Elite_hacker_gang_has_unlimited_supply_of_zero_day_bugs (discussing an elite hacker group's suspected 2010 zero-day attack on Google and other Western companies that Google initially attributed to Chinese hackers).

460 *See* Ryan Gallagher, *Cyberwar's Gray Market*, SLATE (Jan. 16, 2013), http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html ("[T]here are fears that the burgeoning trend in finding and selling exploits is spiraling out of control.").

461 *See, e.g.*, Nate Anderson, *Confirmed: US and Israel Created Stuxnet, Lost Control of It*, ARS TECHNICA (June 1, 2012), http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it (describing how the United States and Israel developed and deployed Stuxnet to attack Iran's nuclear program, but the virus spread to other systems).

be governed because attacks can be linked to a particular country, and because states have an interest in a shared set of rules that protect their combatants as well.[462] The rise of organized armed violence by nonstate actors, such as terrorist groups, challenges the laws of war in ways similar to cyberattacks.[463] Terrorist attacks are harder to link to a particular entity or group, and terrorists are often willing to forgo the protections of the laws of war to more effectively pursue their goals.[464] Cyberattacks are also difficult to attribute, increasing countries' willingness to use them. In addition, some states, such as North Korea, have little to lose from cyber-retaliation, which undercuts adherence to legal rules or norms.[465] There is still no definitive proof, for example, that Russia was responsible for the cyberattacks on Estonia in 2007, or that North Korea was behind the attacks on South Korea and the United States in July 2009.[466]

Where there is armed conflict, there are arms merchants. In previous work, security researcher Oliver Day and I described the market for software security vulnerabilities.[467] That research, though, did not address one increasingly important consumer for exploits: nation-states.[468] A new set of firms, such as Vupen, cater principally to intelligence services; they refuse to share vulnerability information with vendors, preferring to confer an advantage upon their clients.[469] Countries pay better than software companies.[470] These firms amass zero-day exploits for widely used operating

---

462 *See* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 984-92 (2011) (reviewing different standards used to hold cyberattackers more accountable).

463 Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 676-78 (2004) (arguing that the distinction between national security and domestic issues is blurred by new conflicts arising from globalization).

464 Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569, 600-02 (2011).

465 Bambauer, *Conundrum*, *supra* note 26, at 618-19 ("North Korea ha[s] little to lose if the Internet goes offline.").

466 *Id.* at 596-97 ("In both cases, initial judgments that a State (Russia or North Korea) was responsible dissolved into uncertainty in the face of mixed evidence.").

467 *See generally* Bambauer & Day, *supra* note 43.

468 I thank Chris Soghoian for helpful discussion of this point.

469 *See* Andy Greenberg, *Meet The Hackers Who Sell Spies the Tools to Crack Your PC (and Get Paid Six-Figure Fees)*, FORBES (Mar. 21, 2012), http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees.

470 States may offer rewards other than money. The United States obtains confidential vulnerability data from firms in exchange for classified information, among other valuable data. *See* Michael Riley, *U.S. Agencies Said to Swap Data with Thousands of Firms*, BLOOMBERG (June 14, 2013), http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html ("Thousands of technology, finance and manufacturing companies are working closely with U.S. national security agencies, providing sensitive information and in return receiving benefits . . . .").

systems and applications such as Microsoft Windows, Google Chrome, and Adobe Flash.[471] They offer not only information about software weaknesses but also tools to attack them.[472] In the language of security researchers, Vupen and its ilk sell weaponized exploits, and business is good.[473]

While worrisome, companies that sell zero-days are at least subject to some controls. Vupen must obey the laws of France, where it is located.[474] Market pressures and the threat of potential regulation have led the company to declare that it will sell only to customers in NATO countries.[475] By contrast, the *underground* market for zero-day exploits knows no such limits.[476] Eliminating this market is effectively impossible: movements of information are too difficult to detect and interdict. Any proposal to deal with the zero-day problem will necessarily be incomplete, but not valueless.

The open market in zero-day exploits presents four key worries. First, sellers may transact directly with unfriendly buyers. Vupen sells only to NATO countries, but other firms may not be so selective.[477] Indeed, if there are fewer suppliers for non-NATO countries, those countries likely must pay a price premium for access, making them attractive customers. Second, the legitimate market may supply a gray or black market indirectly through secondary transactions. Purchasers of zero-days, for example, may resell them, knowing they are secure against those particular exploits.[478] Third, buyers may involuntarily create risk through a lack of cybersecurity, particularly if zero-day tools are shared widely within the purchasing entity or beyond.[479] For instance, if a national security agency shares exploits with civilian cybersecurity agencies and those civilian agencies' systems are compromised, the zero-days could spread even though the initial purchaser

---

471 *See* Greenberg, *supra* note 469.

472 *See* Naraine, *Vista Exploit Surfaces on Russian Hacker Site*, *supra* note 62.

473 *See, e.g.*, Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits (providing a list of some of the most lucrative prices garnered for zero-day exploits).

474 VUPEN SECURITY, THREAT PROTECTION PROGRAM 1, http://wikileaks.org/spyfiles/files/0/279_VUPEN-THREAD-EXPLOITS.pdf (last accessed Mar. 22, 2014) (listing the company's address in Montpelier, France).

475 Greenberg, *supra* note 469.

476 Bambauer & Day, *supra* note 43, at 1066-68.

477 *See* Gary Davis, *Zero-Day Exploits Provide an Inside Look at the Cybercriminal Black Market*, MCAFEE (Nov. 13, 2012), http://blogs.mcafee.com/consumer/zero-day-exploits-provide-an-inside-look-at-the-cybercriminal-black-market (describing the billion-dollar "Cyber Black Market" and the threat of zero-day exploits).

478 This is an important difference between kinetic attacks and cyberattacks. A party who resells a kinetic weapon faces the risk of attack from it, generating some deterrence for secondary sales. A party with a zero-day can take precautions against it, reducing or eliminating such resale risk.

479 I thank Chris Soghoian for this point.

remains secure.[480] Finally, sellers present attractive targets for hacking and espionage.[481] To someone who wants weapons, burglarizing a gun store likely seems sensible. Vupen's systems are probably more secure than most, but they are not perfect, and a breach of its data could be catastrophic.

Researchers have proposed regulating zero-day exploits as cyberweapons, such as by imposing limits on transactions and exports.[482] These proposals are worth considering and would be consonant with past security efforts. For example, the United States long regulated the export of strong encryption, classifying it as a munition.[483] Regulation, though, faces both legal and practical obstacles. Legally, transactions in information increasingly receive First Amendment protection against governmental regulation.[484] Bans on zero-day sales might pass muster under commercial speech's intermediate scrutiny standard, though sharing source code could potentially draw heightened scrutiny.[485] The recent trend in Supreme Court jurisprudence on laws regulating information is toward skepticism. Though national security constitutes a government interest greater than protecting children from violent video games, blocking emotionally harmful protests at funerals, or

480 *See, e.g.*, Ryan Gallagher, *supra* note 460 (explaining the dangers of an unregulated zero-day exploit market for national governments and agencies).

481 *Cf.* Jaikumar Vijayan, *Vupen Security Denies It's Been Hacked*, COMPUTERWORLD (June 7, 2012), http://www.computerworld.com/s/article/9227875/Vupen_Security_denies_it_s_been_hacked (noting that Vupen "find[s] and exploit[s] unpatched bugs in leading software products," which it then sells "to security vendors, governments, law enforcement agencies and to corporations").

482 *See, e.g.*, Taiwo A. Oriola, *Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities*, 28 J. MARSHALL J. COMPUTER & INFO. L. 451, 521-22 (2011) ("Th[is] paper . . . urges that industry and government should cease patronizing the underground market for vulnerabilities, and penalize illicit vulnerabilities trading."); James Ball, *Secrecy Surrounding 'Zero-Day Exploits' Industry Spurs Calls for Government Oversight*, WASH. POST (Sept. 1, 2012), http://articles.washingtonpost.com/2012-09-01/world/35498227_1_exploits-researchers-security-flaws; Mathew J. Schwartz, *Weaponized Bugs: Time for Digital Arms Control*, INFORMATIONWEEK (Oct. 5, 2012), http://www.informationweek.com/security/attacks/weaponized-bugs-time-for-digital-arms-co/240008564 ("Given the shift from bug bounties to vulnerabilities being used to power digital espionage or offensive operations, why *not* regulate the sale of dangerous bugs?").

483 *See, e.g.*, Thinh Nguyen, Note, *Cryptography, Export Controls, and the First Amendment in* Bernstein v. U.S. Dep't of State, 10 HARV. J.L. & TECH. 667, 671-72 (1997) (stating that an encryption program called "Snuffle" was classified as a "defense item" and placed on the U.S. Munitions List).

484 *See, e.g.*, Sorrell v. IMS Health, 131 S. Ct. 2653, 2659 (2011) (providing First Amendment protection to "[s]peech in aid of pharmaceutical marketing"); *see also* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 63 (2014) ("Together, these principles suggest that state action will trigger the First Amendment any time it purposefully interferes with the creation of knowledge.").

485 *See* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1145 (9th Cir.) ("Nor need we resolve whether the challenged regulations constitute content-based restrictions, subject to the strictest constitutional scrutiny, or whether they are, instead, content-neutral restrictions meriting less exacting scrutiny."), *reh'g en banc granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999). *See generally* Nguyen, *supra* note 483.

preventing animal cruelty, regulation of software code is likely to face searching judicial review.[486]

Regulation of zero-day transactions also faces practical barriers. It may be difficult to identify a zero-day exploit as opposed to other vulnerability information for regulatory purposes, although computer scientists are confident in their ability to define the category.[487] Attempts to regulate the sale of surveillance or censorship technology, for example, have foundered on the problem of defining permitted and prohibited transactions, particularly for dual-use goods.[488] Sellers may not know whether a vendor has knowledge of a particular flaw, and requirements to divulge information to them could undercut the security research market[489] (and possibly constitute a taking if the exploit qualifies as a trade secret[490]). Moreover, intrusive regulation risks driving transactions underground or offshore.[491] Vupen may be obnoxious, but at least it operates overtly. All of these difficulties may be worth tolerating, however, if they increase the cost of malfeasors' access to zero-day exploits.

B. *Partial Defenses*

While a complete defense to zero-day attacks is impossible, policymakers can improve cybersecurity with three regulatory moves: (1) mandatory access to public zero-day markets for the federal government, (2) required confidential reporting on transactions by firms in those markets, and (3) a reward system for researchers who share vulnerabilities with the government.

---

486 *See generally* Brown v. Entm't Merchs. Ass'n, 131 S. Ct. 2729 (2011) (video games); Snyder v. Phelps, 131 S. Ct. 1207 (2011) (funeral protests); United States v. Stevens, 559 U.S. 460 (2010) (animal cruelty).

487 *See generally, e.g.*, Lajos Nagy, Richard Ford & William Allen, *N-Version Programming for the Detection of Zero-Day Exploits* (Apr. 2006) (paper presented at the IEEE Topical Conference on Cybersecurity), *available at* https://www.cs.fit.edu/media/TechnicalReports/cs-2006-04.pdf (using an auction web application to show resilience to non-zero-day vulnerabilities, in an effort to detect zero-day attacks).

488 *See* Derek Bambauer, *Cool Tools for Tyrants*, LEGAL AFF. (Jan.–Feb. 2006), http://www.legalaffairs.org/issues/January-February-2006/feature_bambauer_janfeb06.msp (explaining how attempts to regulate each technology have given rise to ambiguous and vague crimes in nations like China).

489 *See* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention* (stating that research is a "risky process" and removing this risk has the potential to foster inefficiency and misallocation since "the profitability of invention requires a nonoptimal allocation of resources"), *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC SOCIAL FACTORS 609, 616-17 (1962).

490 *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 987 (1984) (holding that intangible property, to the extent it constitutes a trade secret, is subject to the Fifth Amendment's Takings Clause).

491 Bambauer & Day, *supra* note 43, at 1067-68.

Congress should pass legislation to implement these measures, and the United States should move to convert unknown unknowns to known unknowns.

First, firms that transact in software security vulnerabilities should be required to permit the federal government to participate in any offerings or services they provide, on nondiscriminatory terms. If Vupen, for example, sought to sell zero-day exploits to France's security services, but not to the United States' NSA, that would be problematic. Software security firms should be legally bound to provide paid access to the U.S. government as a necessary condition of continued operation. This would enable the government to develop and deploy countermeasures to at least some zero-day attacks.

Congress has taken analogous measures for other potential risks to national security. For example, one cannot obtain a patent for inventions in nuclear materials or weapons,[492] but such inventions are eligible for a governmental reward scheme.[493] And, the statute transfers rights to the invention from the inventor to the federal government.[494] Similarly, export controls restrict private firms' ability to engage in transactions with foreign countries. One may not transfer software utilizing encryption to countries such as Iran or North Korea,[495] and one may not sell certain supercomputers to countries such as China or Russia.[496] These rules apply to all firms within U.S. jurisdiction. Thus, Congress has either mandated or forbidden certain transactions based on national security concerns and could mount a similar effort for zero-day sales.

Not all zero-day merchants fall under U.S. jurisdiction or enforcement. Even those operating abroad, however, likely have contacts with the United States. Vupen's employees, for example, visit the United States.[497] Many, if not all, such firms use financial or payment processing companies that are

---

492 *See* 42 U.S.C. § 2181(a) (2006) ("No patent shall hereafter be granted for any invention or discovery which is useful solely in the utilization of special nuclear material or atomic energy in an atomic weapon."); Michael Risch, *Everything Is Patentable*, 75 TENN. L. REV. 591, 595 n.22 (2008).

493 *See id.* § 2187(b)(3) (explaining the royalty-fee reward system for nuclear-related inventions).

494 *See id.* § 2183 (providing the Nuclear Regulatory Commission with a license to use any such product that receives a patent).

495 *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 437-41 (2012) (providing a history of the restrictions of the U.S. encryption export regime). *See generally* U.S. Dep't of Commerce, *Advisory Opinion: Downloads of Encrypted Software Reviewed and Classified as "Mass Market"* (Sept. 11, 2009), *available at* http://www.bis.doc.gov/index.php/policy-guidance/advisory-opinions (click document title link) (prohibiting the knowing dissemination of encryption software to Iran, Cuba, Syria, Sudan, and North Korea).

496 15 C.F.R. § 740.7 (2013) (creating a tiered system by which certain levels of supercomputers are prohibited from being exported to certain nations).

497 Vupen, *Upcoming Events to Meet the VUPEN Team*, http://www.vupen.com/english/events.php (last visited Mar. 22, 2014) (listing upcoming corporate events in Florida, Nevada, and Washington, D.C.).

subject to U.S. regulation. Some software companies, such as Microsoft, are eager to access U.S. government data on vulnerabilities and threats and have demonstrated a willingness to provide the NSA with exploit information before making it public.[498] These links provide potential leverage. Congress could attach provisions to this legislation that would allow the executive branch to designate firms that do not provide access to the government and to require banks and payment processors to forgo transactions with them.[499] Analogous measures have been implemented to interdict financing for terrorist groups[500] and have been proposed to deal with websites illegally offering prescription drugs or copyrighted works.[501]

Second, Congress should mandate a transaction-reporting system for firms trading in vulnerabilities. These companies should have to report, on a confidential basis, the purchaser's identity in all transactions of zero-day exploits to the NSA. This data would remain confidential and should be designated as statutorily immune from discovery or other use unless the NSA expressly chooses to share it.[502] The statute should enable auditing of firms' records by the NSA if the Agency is able to demonstrate an objectively reasonable basis to suspect inaccuracies or falsification. To make this provision less objectionable for the vulnerability merchants, Congress should include payments to the reporting firms. While additional spending

---

498 *See* Sean Gallagher, *NSA Gets Early Access to Zero-Day Data from Microsoft, Others*, ARS TECHNICA (June 14, 2013), http://arstechnica.com/security/2013/06/nsa-gets-early-access-to-zero-day-data-from-microsoft-others (detailing information swaps between the NSA and Microsoft, among other government agencies and private corporations).

499 *See* David Adams, *Analysis: U.S. Sanctions Make Cuba's Bank Account Too Toxic for Banks*, REUTERS (Nov. 29, 2013), http://www.reuters.com/article/2013/11/29/us-cuba-usa-banking-analysis-idUSBRE9AS0QE20131129. This threat is significant. After MasterCard, Visa, Discover, and PayPal ceased processing payments to WikiLeaks, its revenues fell by 95%. Yochai Benkler, *A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 339-42 (2011) (explaining that Senator Lieberman requested that U.S. companies cut financial ties with WikiLeaks—a request with which they complied).

500 *See, e.g.*, Exec. Order 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001) (imposing penalties on those engaging in or otherwise supporting terrorism).

501 *See, e.g.*, Stop Online Piracy Act, H.R. 3261, 112th Cong. § 101(21)(B) (2011) (seeking "[t]o promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property," including copyrighted works); Mathea Falco & Philip Heymann, *Fighting the Online Drug Corner*, WASH. POST (Mar. 15, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/03/14/AR2008031403018.html (arguing that "credit card companies and their sponsoring financial institutions should prohibit the use of their services for illicit sales of controlled substances," specifically prescription drugs).

502 *Cf.* Bambauer, *Cybersieves*, *supra* note 177, at 434-35 (describing disclosure requirements for "collect[ed] information about civil judgments, settlements, and [certain] criminal convictions against physicians and health care providers" that is not accessible by the general public but is accessible to regulators).

is politically difficult, this expenditure would be a small but worthwhile investment in security.

Similar reporting systems are widely used to mitigate risk. NASA, for example, encourages confidential reporting of "near-miss incidents"—those that nearly resulted in aviation mishaps—to improve safety procedures and detect product defects.[503] Similarly, insurers offering policies for medical malpractice liability must report judgments and settlements to the National Health Practitioner Data Bank.[504] This malpractice information is available for use by state medical licensing boards and federal agencies, but is otherwise confidential.[505] In addition, the Federal Railroad Administration is testing a Confidential Close Call Reporting System to identify risks in rail operations via confidential reporting of near-miss incidents.[506] The Department of Veterans Affairs has a similar reporting system for patient safety.[507] And finally, the Federal Communications Commission has one for network outages.[508] Thus, the federal government already has well-established confidential reporting systems to help manage risk.

A zero-day reporting system has several benefits. It would enable the government to detect problematic sales, particularly to unfriendly states and insecure parties. It would increase the effectiveness of countermeasures that mitigate zero-day exploits by providing a rough guide to how widely distributed a particular attack tool is. It would allow the government to identify whether firms follow their stated criteria for sales (such as Vupen's self-imposed limit to NATO countries and clients) and to scrutinize suspect firms more closely. Lastly, it would provide a crude estimate of the ebb and flow of zero-day threats and of the platforms and applications viewed by the merchant as worthy of attention (and payment).

Finally, Congress should authorize a "bug bounty" program.[509] Its goal would be to collect zero-day exploits and encourage researchers to sell their

---

503 *Aviation Safety Reporting System*, NASA, http://asrs.arc.nasa.gov/ (last visited Mar. 22, 2014).

504 42 U.S.C. § 11131 (2006) (requiring reports on medical malpractice payments).

505 *Id.* § 11137 (listing exceptions to confidentiality).

506 *Introduction: Confidential Close Call Reporting System*, BUREAU TRANSP. STAT., http://www.c3rs.bts.gov/index.htm (aiming to allow citizens and railworkers to report "a close call" online).

507 *VA National Center for Patient Safety*, U.S. DEP'T OF VETERANS AFF., http://www.patientsafety.va.gov/media/reporting.asp (last visited Mar. 22, 2014) (describing the Patient Safety Information System—an "internal, confidential, non-punitive system" used to document patient safety).

508 *Network Outage Reporting System (NORS)*, FCC, http://transition.fcc.gov/pshs/services/cip/nors/nors.html (describing a "web-based filing system" to report "significant disruptions or outages" in communication networks).

509 Kim Zetter, *With Millions Paid in Hacker Bug Bounties, Is the Internet Any Safer?*, WIRED (Nov. 8, 2012), http://www.wired.com/threatlevel/2012/11/bug-bounties (explaining how the "Google

findings to the U.S. government rather than to private firms or other nation-states. A government agency, such as the NSA or the U.S. Computer Emergency Readiness Team (CERT), should be provided funds to buy zero-day vulnerability information.[510] The entity selling the exploit, such as a security research firm, would have to certify under penalty of perjury that it had not previously shared the vulnerability information with others and would have to agree contractually not to do so in the future.[511] Congress should consider backing these requirements with substantial criminal penalties as it has done in other contexts.[512] Arms dealers who sell to both sides are held in low esteem.

Similar private bounty programs implemented by Google and Mozilla have had considerable success in identifying and remediating bugs.[513] The funding and amount paid per bug should be generous: removing zero-days from the Internet ecosystem is highly beneficial. Moreover, generous payments will have further positive effects. First, these payments will spur researchers to search for additional bugs. These bugs are like latent defects in a product—they lurk, creating risk, until they are discovered. Second, paying above-market rates makes it more difficult for others to purchase zero-days. Pushing others out of the zero-day market is useful both offensively and defensively. Offensively, accumulating zero-days provides the United States with the building blocks for future Stuxnets. Defensively, it reduces the likelihood that U.S. firms or government entities will fall victim to attack.

However, the bug bounty program will create several challenges. First, price: more competition for zero-day exploits will drive up their cost. This increase will burden the public fisc slightly but will incentivize bug research. Second, the government will need to decide how to use exploit information. Congress could establish rules for what the NSA may do with the data, or it

---

Pwnium" contest has been used successfully to encourage hackers to "bug hunt" for companies rather than for the black market).

510 *Cf.* Bambauer & Day, *supra* note 43, at 1102-03 (suggesting CERT as a clearinghouse for vulnerabilities).

511 *Cf. Zero Day Initiative*, TIPPINGPOINT, http://www.zerodayinitiative.com/about (last visited Mar. 22, 2014) (requiring "researchers [to] provide TippingPoint with exclusive information about previously un-patched vulnerabilities").

512 *Cf.* 18 U.S.C. § 175 (2012) (outlining serious penalties for possession of biological weapons).

513 Thomas Claburn, *Google Ups Bug Bounties Amid Booming Exploit Market*, INFORMATIONWEEK (Aug. 16, 2012), http://www.informationweek.com/security/management/google-ups-bug-bounties-amid-booming-exp/240005721 (explaining Google's and Mozilla's successful reward systems for vulnerability disclosure, including two $60,000 Google payments for impressive finds); Dennis Fisher, *Behind the Numbers of Mozilla's Bug Bounty Program*, THREATPOST (Sept. 28, 2011), http://threatpost.com/behind-numbers-mozillas-bug-bounty-program-092811/75701 (finding that the number of bug reports received by Mozilla has dropped significantly since the implementation of bug bounty programs).

could defer to the Agency (and, by extension, the executive branch) to make that decision. If the Agency uses the exploits to build cyberweapons, such as Stuxnet, or enables others to do so, it is likely to share vulnerability information less widely than it would without a vision of offensive use. If the Agency enables other government entities or private firms to safeguard against the zero-days, it risks having those patches shared, including with potential targets. There is also an ironic feedback effect: the more important the vulnerability, the greater the temptation to weaponize it, and thus withhold it from other affected parties.

The hardest decision regarding sharing is determining whether to notify the affected vendor.[514] This Article argues that telling the vendor about the vulnerable code should be the default practice, with two caveats. First, the NSA should work with the vendor to ensure the patch for the vulnerability is maximally effective and minimally visible. If the company draws attention to the patch's criticality, it may signal to anyone who has independently discovered it that the window of vulnerability is closing, which could draw attacks.[515] Second, the NSA should work with the vendor to include detection code in its patches. This would help the Agency estimate how often vulnerabilities are discovered independently, and perhaps to detect double-dealing by researchers participating in the bug-bounty system.[516]

This Article's solutions for the zero-day problem—the unknown unknowns—differ in character from those for vulnerabilities with existing solutions (the known unknowns) in that they have a greater focus on prevention. Mitigation is still invaluable: disaggregation and heterogeneity are just as helpful for zero-days as for known bugs. Preventive steps, however, are more important for zero-day exploits than for known bugs. With known vulnerabilities, defenses are possible, though logistically constrained by externalities, information costs, and system complexity. With

---

514 *See* Bambauer & Day, *supra* note 43, at 1089-90 (arguing for legislation that would create a safe harbor for researchers when they report a vulnerability to the vendor before publishing such information).

515 Ashish Arora, Anand Nandkumar & Rahul Telang, *Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis*, 8 INFO. SYS. FRONTIERS 350, 355 (2006) (finding that vulnerabilities are either "secret, published, or patched" and that a vulnerability can be a secret but still continue to get exploited (emphasis removed)).

516 *See* Andy Ozment, Vulnerability Discovery & Software Security 88-95 (Aug. 31, 2007) (unpublished Ph.D. dissertation, University of Cambridge), *available at* http://www.andyozment.com/papers/ozment_dissertation.pdf (explaining the role of independent discovery in detecting vulnerabilities and finding that often, multiple researchers independently find the same vulnerability).

zero-days, however, defenses are impossible.[517] Defenders must rely solely on mitigation and recovery. While prevention tends to be overrated in cybersecurity literature, it remains useful in practice. In particular, even if complete prevention is impossible, defenders may be able to reduce an exploit's effects—for example, by allowing a server to terminate an affected program, rather than having it cause the server to crash. This is similar to a public health approach: even if we cannot prevent people from contracting a virus, we may be able to make it less lethal.[518] Thus, the three-part agenda above seeks to increase America's access to information about zero-days, thereby enabling precautions and improving mitigation.

CONCLUSION

Something terrible is going to happen in cyberspace. That may be useful for cybersecurity.

The United States suffers significant but less visible cyberattacks daily. Complex technology, mixed with victims' reluctance to disclose the scale of harms, leads to an underappreciation of cyber-risks. This disjunction generates the ongoing puzzle of cybersecurity: the gap between the dramatic assessment of the risks the United States faces and the minimalist measures the country has taken to address them. America's predictions do not match its bets. One of these positions is wrong.

But the economic and structural factors that impede regulation suggest reform will not occur without a dramatic focusing event.[519] The United States did not address its educational deficiencies in math and science until the Soviets launched Sputnik into orbit.[520] Until the near-meltdown at Three Mile Island, America was complacent about nuclear energy safety.[521] And it took the attacks of 9/11 for the country to address the rise in international terrorism, the gaps in its intelligence systems, and the weaknesses in

---

517 Kesan & Hayes, *supra* note 46, at 474 (using the term "mitigative counterstriking" to define the core concept of an "active defense" that will not eliminate the threat but rather mitigate its effects).

518 *See* Sales, *supra* note 35, at 1539-44 (describing the multifaceted public health approach that includes inoculation, biosurveillance, and isolation and quarantine—a model that can be mirrored in a cybersecurity approach).

519 *Cf.* JOHN W. KINGDON, AGENDAS, ALTERNATIVES, AND PUBLIC POLICIES 165 (1984) (noting that it often takes a large event such as rumored regulation or deregulation, turf disputes over jurisdiction, or some other form of interagency "strife" to drive change).

520 Cornelia Dean, *When Science Suddenly Mattered, in Space and in Class*, N.Y. TIMES, Sept. 25, 2007, at F4 (explaining how the launch of Sputnik was used by scientists and researchers as a "warn[ing to] Congress that the cold war was being fought with slide rules, not rifles").

521 PERROW, *supra* note 88, at 15-31 (describing, in detail, the hydrogen explosion that spurred subsequent nuclear safety policy and cooled nuclear factory construction across the United States).

aviation security.[522] This Article's role is to sit on the shelf, awaiting that focusing event with dread. When it occurs, regulators will need a model for a response. This Article offers one.

Cybersecurity offers copious challenges for future research. Two are particularly relevant to this Article. First, data integrity is a difficult puzzle. Restoring data after attacks is unhelpful if one cannot tell good information from bad—we must be able to distinguish authorized updates from unauthorized ones. This seemingly technical puzzle has important implications for provenance in other areas, from rules of evidence to intellectual property, which struggle with similar authentication problems.

Second, nation-states are now engaged in the long twilight struggle of espionage and hacking in cyberspace. At present, there are neither formal rules nor tacit norms that govern conduct. Eventually, though, countries must arrive at accommodations. Spying,[523] assassination,[524] and armed combat[525] all benefited from shared rules, even during the Cold War. Lawyers can raise awareness of these benefits and help shape the system that emerges. Future research can contribute to both of these inquiries.

For now, ghosts roam the network. They cannot be driven out. We must lessen the effects of their touch.

---

522 THOMAS H. KEAN ET AL., THE 9/11 COMMISSION REPORT 254-65 (2004) (explaining how executive agencies received many warnings of "near term 'spectacular' terrorist attacks" prior to 9/11, but from a defense standpoint, "[f]ar less was done domestically" than internationally).

523 *See generally* Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321 (1996) (analyzing the evolution of international espionage law in times of war).

524 *See generally* Nathan A. Sales, *Self-Restraint and National Security*, 6 J. NAT'L SECURITY L. & POL'Y 227, 249-51 (2012) (describing the U.N. Charter rules pertaining to peacetime killings).

525 *See generally* Geoffrey S. Corn, *Back to the Future: De Facto Hostilities, Transnational Terrorism, and the Purpose of the Law of Armed Conflict*, 30 U. PA. J. INT'L L. 1345, 1346-47 (2009) (stating that the "triggering paradigm" that spurs armed conflict has evolved with the growth of the United States and the development of the Laws of Armed Conflict).