Article

Conundrum

Derek E. Bambauer†

† Associate Professor of Law, Brooklyn Law School. The author thanks Lia Sheena, Lia Smith, and Carolyn Wall for expert research assistance. Thanks for helpful suggestions and discussion are owed to Fred Bloom, Susan Brenner, Herbert Burkert, Mike Carroll, Anupam Chander, Kate Coyer, Oliver Day, Ron Deibert, Lauren Gelman, Alex Glashausser, Eric Goldman, James Grimmelmann, Jim Harper, Dan Hunter, Jeff Jackson, Margo Kaplan, Rebecca Kysar, David Levine, Andrew Lewman, Tom Lin, Andrea Matwyshyn, Alana Maurushat, Jason Mazzone, Bill Merkel, Milton Mueller, Thinh Nguyen, Paul Ohm, Nelson Tebbe, Marketa Trimble, Ben Trachtenberg, Stefaan Verhulst, Jane Yakowitz, Jonathan Zittrain, the participants in the Cybersecurity Workshop at Central European University, the participants in the faculty workshop at Washburn University School of Law, the participants in the Boston University School of Law Works-in-Progress Intellectual Property Colloquium, the participants in the Santa Clara University School of Law Internet Law Works In Progress Series, and the participants in the U.S. Department of State's Conference on Balancing Free Expression and Security in Cyberspace. The author thanks the Dean's Summer Research Stipend Program, Dean Michael Gerber, and President Joan Wexler, at Brooklyn Law School, for financial support. The author welcomes comments at <derek.bambauer@brooklaw.edu>.

> Time and accident are committing daily havoc on the originals deposited in our public offices. The late war has done the work of centuries in this business. The lost cannot be recovered, but let us save what remains; not by vaults and locks which fence them from the public eye and use in consigning them to the waste of time, but by such multiplication of copies, as shall place them beyond the reach of accident.
>
> Letter from Thomas Jefferson to Ebenezer Howard (Feb. 18, 1791), *in* 3 THE WRITINGS OF THOMAS JEFFERSON 211, 211 (H.A. Washington ed., 1871).[1]

INTRODUCTION

A cyberattack was causing Iran's uranium-enrichment centrifuges to secretly malfunction. The devices, responsible for concentrating uranium gas to produce a weapons-grade version of the element, were spinning too fast, based on incorrect instructions from their computer controllers.[2] Simultaneously, those computers were sending reassuring data back to the Iranian engineers monitoring them, painting a false picture of normal operation.[3] Over time, the centrifuges' rotors began to wobble, destroying some of the machines and damaging others.[4]

1. I thank Bill Merkel for this quote.

2. William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1.

3. Christopher Williams, *Western Power Created Virus to Sabotage Iran's Nuclear Plans*, DAILY TELEGRAPH (London), Jan. 22, 2011, at 20.

4. Mark Clayton, *Stuxnet Attack on Iran Nuclear Program Came About a Year Ago, Report Says*, CHRISTIAN SCI. MONITOR (Jan. 3, 2011, 4:53 PM), http://

The concealed overspin set back Iran's efforts to acquire nuclear weapons by at least three years, according to American and Israeli intelligence sources.[5] The cause: the most sophisticated cyberweapon yet created, known as Stuxnet. Engineered to activate its payload only when operating within Iran's enrichment system,[6] Stuxnet recorded normal operating data, sped up the rotors, and then fed the recorded data back to the controllers. It was the ultimate stealth assault.

Stuxnet succeeded where conventional efforts to delay Iran's nuclear ambitions—from diplomacy to threats of force—had failed.[7] Moreover, the superworm operated with utter deniability: although it seems clear that the cyberattack resulted from a joint Israeli-American operation, there is no concrete evidence to link the two countries to Stuxnet.[8] The hack damaged Iran's atomic program to roughly the same degree that a conventional airstrike would have,[9] but without killing Iranian personnel and revealing the (likely Israeli)[10] identity of the country launching the military attack. From the U.S. perspective, this was the perfect kill: an attack that badly hurt Iran's nuclear enrichment regime, with no human casualties, no harm to America's international image, and no evidence to point conclusively to Stuxnet's creators. Exploiting an Iranian cybersecurity weakness proved enormously valuable and perfectly deniable. Stuxnet demonstrates vividly the power of cyberweapons and the risks of inadequate cybersecurity.

Cybersecurity is a conundrum. Scholars, government officials, journalists, and computer scientists all agree that inade-

www.csmonitor.com/USA/2011/0103/Stuxnet-attack-on-Iran-nuclear-program-came-about-a-year-ago-report-says.

5. Broad et al., *supra* note 2.

6. Kim Zetter, *Report: Stuxnet Hit 5 Gateway Targets on Its Way to Iranian Plant*, WIRED (Feb. 11, 2011, 8:05 PM), http://www.wired.com/threatlevel/2011/02/stuxnet-five-main-target/.

7. *See, e.g.*, Richard A. Falkenrath, Op-Ed., *From Bullets to Megabytes*, N.Y. TIMES, Jan. 27, 2011, at A31 ("A sophisticated half-megabyte of computer code apparently accomplished what a half-decade of United Nations Security Council resolutions could not.").

8. Broad et al., *supra* note 2.

9. *See The Unconventional Attack on Iran*, MISSINGPEACE (Nov. 29, 2010, 3:20 PM), http://missingpeace.eu/en/2010/11/the-unconventional-attack-on-iran (explaining that, because of the potential for reactor meltdown, "Stuxnet could even be more effective than an airstrike").

10. Christopher Williams, *Israeli Security Chief Celebrates Stuxnet Cyber Attack*, THE TELEGRAPH (Feb. 16, 2011, 7:00 AM), http://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html.

quate security is an emerging threat—perhaps even a catastrophic one—and that preventive action is urgently needed. However, no one can agree on precisely what cybersecurity means, or requires. Presidential task forces have recommended widespread changes to safeguard America's cyber-systems;[11] scores of bills have been introduced in Congress;[12] international treaties have been mooted.[13] By most accounts, the virtual sky is about to fall. Yet, despite nearly a decade of sustained attention, little, if any, cybersecurity progress has occurred.

This Article argues that the current failure to meaningfully address this problem occurs because cybersecurity is undertheorized: it is, at best, poorly defined, and it lacks a coherent framework to guide change. Current scholarship on cybersecurity is moored in doctrinal models that both misdiagnose the relevant issues and offer answers that would badly damage the net's innovative capacity. Drawing upon scholarship in economics, behavioral biology, and mathematics, this Article seeks to remedy these shortcomings with a theoretical model oriented around information, in distinction to the near-obsession with technological infrastructure demonstrated by contemporary scholars. This information-based approach to cybersecurity, which focuses on access and alteration of data and on guaranteeing its integrity, can remediate critical threats.

To implement the theory's recommendations, this Article suggests, counter intuitively, that creating *in*efficient storage and network connections best protects cybersecurity. Moreover, it points out clearly that cybersecurity policy necessitates difficult tradeoffs, particularly between ensuring authorized access and alteration and preventing unauthorized interaction with data. This Article outlines implementation through legislation that requires inefficient data storage for entities holding critical information, mandates testing that redundant storage, and invests in transitioning organizations to the new regulatory re-

11. *See generally* Bill Lane, *Cyber Security and Communications*, Fed. Commc'ns Comm'n, http://www.fcc.gov/pshs/techtopics/techtopics20.html (last visited Nov. 7, 2011) (listing presidential directives and task force efforts).

12. *See, e.g.*, Gautham Nagesh, *Senators Debate Terms of Cybersecurity Overhaul*, THE HILL (June 29, 2010, 10:33 AM), http://thehill.com/blogs/hillicon-valley/technology/106119-senators-debate-terms-of-cybersecurity-overhaul (describing three different bills addressing cybersecurity concerns).

13. *See, e.g.*, John Markoff, *Steps Taken to End Impasse Over Cybersecurity Talks*, N.Y. TIMES, July 17, 2010, at A7 (describing a set of cybersecurity recommendations that mark steps toward a resolution of American opposition to a Russian-proposed treaty on cybersecurity).

gime. Next, it describes regulation that generates inefficient network connectivity by subsidizing interconnection, maintaining links between network providers during disputes, and exploring research into heterogeneous routing as a last-resort option. Lastly, this Article describes the stakes in cybersecurity debates: adopting current scholarly approaches risks jeopardizing not only the architecture that makes the Internet a potent medium for innovation and communication, but also key American normative commitments to free expression on-line.

This Article, to be plain, is a significant departure from the conventional academic wisdom on cybersecurity. Contemporary scholarly efforts on the topic remain rigidly locked into familiar doctrinal models, particularly public international law,[14] the law of armed conflict,[15] and criminal law.[16] While scholars admit that cybersecurity fits poorly in these conceptual boxes, they nevertheless seek to remold its challenges to fit their tools.[17] Thus, the dominant analytical mode for cybersecurity concentrates heavily on the identity and intent of the malicious actor. Susan W. Brenner notes that cybercrime and cyberterrorism encompass similar actions—"only the motivation differs."[18] Kelly A. Gable classifies cyberterrorism by intent, as

14. *See, e.g.*, Jeffrey Hunker, *U.S. International Policy for Cybersecurity: Five Issues that Won't Go Away*, 4 J. NAT'L SECURITY L. & POL'Y 197, 212 (2010) ("Looking toward existing international regimes that have parallels to cyber seems a useful way of gaining insight into what an international cybersecurity regime might look like.").

15. *See, e.g.*, Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 190 (2006) ("It is both necessary and appropriate that the same principles of international law intended to regulate conventional armed conflict and reduce its adverse effects apply to information warfare."). *See generally* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY. L. & POL'Y 87 (2010) (discussing how the law of war might apply to cyberattacks).

16. *See, e.g.*, Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 203 (2006) (examining familiar doctrinal models such as "leaving the burdens of cyber-crime on victim companies, of placing it upon the software and hardware manufacturers, of expanding the role of governmental regulation, and of a combination of all three options").

17. *See, e.g.*, Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 379 (2007) (stating that the "speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult" (quoting DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE viii (2003) [hereinafter NATIONAL STRATEGY TO SECURE CYBERSPACE], *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf)).

18. *Id.* at 399.

crime "with the purpose of coercing a government to alter its policies."[19] Sean Watts identifies state affiliation as "an irreducible minimum of lawful participation in CNA [computer network attacks]."[20] Matthew J. Sklerov notes that the "current legal paradigm . . . requires attribution to a state or its agents."[21] Stephen Dycus states that lack of attribution undercuts deterrence and a state's ability to respond to an attack.[22] Richard A. Clarke and Robert A. Knake focus on attribution and its attendant challenges, particularly in proving that a state is the perpetrator of a cyber-threat.[23] Eric T. Jensen describes the "inability to attribute cyber attacks"[24] as a "significant problem that plagues cybersecurity,"[25] and that "complicate[s] a state's response" to an attack.[26] Milton L. Mueller proposes a new, distributed, peer-produced governance model to deal with "difficult-to-trace actions and distributed actors and attacks that easily cross national borders."[27] Attributing Internet actions to a particular actor, and discerning their motivations, is essential for these scholars to employ preexisting doctrinal responses.

However, attribution of a cyberthreat to a particular actor on the Internet—to say nothing of divining that actor's intent—is highly difficult given the network's open, anonymous, distributed architecture.[28] Unsurprisingly, then, nearly all scholars

19. Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 62–63 (2010) (citing BERNADETTE SCHELL & CLEMENS MARTIN, WEBSTER'S NEW WORLD HACKER DICTIONARY 87 (2006)).

20. Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391, 396 (2010).

21. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States* W*ho Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 7 (2009).

22. Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155, 163–64 (2010).

23. RICHARD A. CLARKE & ROBERT A. KNAKE, CYBER WAR 214–15, 248–52 (2010).

24. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1538 (2010).

25. *Id.*

26. *Id.* at 1542.

27. MILTON L. MUELLER, NETWORKS AND STATES 182 (2010).

28. *See, e.g.*, Dycus, *supra* note 22 (arguing that the "difficulty identifying the source of a cyber attack" renders traditional deterrence-based policies of retaliation impractical); Gable, *supra* note 19, at 102 (discussing how the ease of "spoofing" IP addresses allows cyberterrorists to "manipulate and obfuscate" their true points of origin, limiting the usefulness of point-of-attack attribution in assigning blame for cyberterrorist attacks).

seek to redesign the Internet to improve attribution. By making it possible, if not mandatory, for data to be linked to its source, this proposed change would enable legal scholars to remain comfortably within familiar modes of analysis. Forcing cybersecurity into these traditions, though, has significant negative effects. Requiring attribution undercuts the innovative architecture of the Internet—what Jonathan L. Zittrain terms its "generativity."[29] It confers greater control on authoritarian regimes that seek to censor speech, such as China and Iran.[30] And it threatens to shift Americans away from shared normative commitments to open communication as a powerful democratizing force.[31] Current scholarship, in short, would destroy the Internet in a futile attempt to save it. This Article proposes a better path.

This Article proceeds in six parts. In Part I, it describes the difficulties that previous scholars and policymakers have encountered when attempting to define a theoretical model for cybersecurity, and how they have reacted by attempting to force it into existing but ill-fitting paradigms such as international law, the law of armed conflict, and criminal law. This Article describes how this lack of vision produces a dangerous policy agenda: altering the Internet's fundamental design to require attribution of communications. Next, Part II catalogues the apocalyptic descriptions of cybersecurity risks, which create a rush to regulate that is likely to be even more harmful than the chimerical horrors of the risks themselves. Part III draws upon analogous scholarship in behavioral biology, economics, and mathematics to produce a radical, insightful new approach to cybersecurity that is oriented around information. It argues that an information-based approach requires focusing on the positive and negative aspects of information access and alteration, with second-order considerations of guaranteeing data integrity. This Article then applies the new theoretical model to

29. Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 2030–31 (2006).

30. *See generally* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (Ronald Deibert et al. eds., 2008) (discussing the history and practice of State Internet filtering around the world).

31. Secretary of State Hillary Clinton's speech on Internet freedom on February 15, 2011, is but the latest exemplar. Hillary Rodham Clinton, U.S. Sec'y of State, Address at George Washington University, Internet Rights and Wrongs: Choices & Challenges in a Networked World (Feb. 15, 2011), *available at* http://www.state.gov/secretary/rm/2011/02/156619.htm (discussing state interference with the Internet during protests in Iran and Egypt and calling for a global commitment to Internet freedom).

generate a surprising solution to positive issues of access and alteration: inefficiency as defense. (The next article in this cybersecurity project will address the negative aspects of access and alteration.) Part IV details how regulation can achieve helpful inefficiency in redundant data storage and network connectivity, and the tradeoffs this prescription creates for preventing unauthorized access and alteration. In Part V, this Article examines how cybersecurity may fundamentally shift American normative commitments to open communication online, and the risks this creates as authoritarian states employ security as a pretext for restricting free expression. This Article concludes by describing the new theory's emphasis on resilience, the limits of law as a cybersecurity tool, and other contexts in which inefficiency confers benefits.

Solving cybersecurity's conundrum requires a new theoretical approach that prizes information over infrastructure. This Article shows us how to do that.

I. WHAT IS CYBERSECURITY?

Conceptualizing cybersecurity challenges policymakers and academics.[32] The current theoretical approaches to cybersecurity, though, have proved to be significantly flawed. They employ definitions that are vague and overbroad; they seek to force cybersecurity's issues into the straitjackets of existing doctrines poorly suited to cybersecurity's problems; and they produce concomitant policy recommendations that not only fail to mitigate, but actually worsen, the Internet's security challenges.

Conventional wisdom on cybersecurity identifies the problem as all-encompassing.[33] Scholars, government officials, and journalists tend to view cybersecurity as the "protection of all things Internet"[34]—an approach that impedes practical progress by failing to set priorities. Government efforts at capturing cybersecurity's scope have been particularly overbroad.

32. The term cybersecurity suffers from what Thomas S. Kuhn calls "incommensurability": although different actors employ the same word, it carries divergent meanings, assumptions, and value structures for each of them. THOMAS S. KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS 148–49 (3d ed. 1996).

33. *See* Peter Sommer & Ian Brown, *Reducing Systemic Cybersecurity Risk*, ORGANISATION FOR ECON. CO-OPERATION & DEV., 9–14 (Jan. 14, 2011), http://www.oecd.org/dataoecd/57/44/46889922.pdf (tracing the history of cybersecurity threats and concerns).

34. Jill R. Aitoro, *Cybersecurity*, NEXTGOV (Oct. 1, 2008), http://www.nextgov.com/the_basics/tb_20080523_5125.php.

President Barack H. Obama's Cyberspace Policy Review offers a representative definition, where cybersecurity is:

> strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.[35]

Presidential policies have been strikingly consistent. President Barack Obama's approach to cybersecurity is almost identical to the Comprehensive National Cybersecurity Initiative (CNCI), the strategy employed by Obama's Republican predecessor, President George W. Bush.[36] Their cybersecurity definitions and programs are closely aligned; indeed, Richard Clarke and Robert Knake call Obama's plan "CNCI redux."[37] Both policies build on the recommendations and definitions (in particular, of critical infrastructure) of President William J. Clinton's Commission on Critical Infrastructure Protection.[38] Regardless of political affiliation, American Presidents have taken an expansive view of cybersecurity.

Proposed federal legislation is equally capacious in approach. The National Cyber Infrastructure Protection Act of 2010 defines "cyber security activities" as:

---

35. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 2 (2010) [hereinafter CYBERSPACE POLICY REVIEW], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

36. *See* Nat'l Sec. Council, *The Comprehensive National Cybersecurity Initiative*, THE WHITE HOUSE, 1, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last visited November 7, 2011) (stating that Obama's policies "build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008").

37. CLARKE & KNAKE, *supra* note 23, at 118.

38. THE PRESIDENT'S COMM. ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 3 (Oct. 1997), *available at* http://www.fas.org/sgp/library/pccip.pdf (defining critical infrastructures as those that are "so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security"); *see* William J. Clinton, *Presidential Decision Directive 63/NSC-63* (May 22, 1998), *reprinted in* BRIAN T. BENNETT, UNDERSTANDING, ASSESSING, AND RESPONDING TO TERRORISM: PROTECTING CRITICAL INFRASTRUCTURE AND PERSONNEL app. 2.2, at 88–99 (2007) (defining critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government").

> a class or collection of similar cyber security activities by a Federal agency that involves personally identifiable data that is—
>
> (A) screened by a cyber security system outside of the Federal agency . . .
>
> (B) transferred, for the purpose of cyber security, outside such Federal Agency; or
>
> (C) transferred, for the purpose of cyber security, to an element of the intelligence community.[39]

The Act conceives of cybersecurity not only broadly—it could include the Federal Trade Commission's anti-spam efforts, for example—but recursively.[40] The Protecting Cyberspace as a National Asset Act of 2010 defines "information security" as "protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide" integrity, confidentiality, and availability.[41] The Homeland Security Cyber and Physical Infrastructure Protection Act of 2011 proposes cybersecurity requirements that cover "an occurrence that jeopardizes the security of data or the physical security of a computer network owned or operated by a Federal agency or covered critical infrastructure,"[42] where critical infrastructure includes private sector computer systems identified by the Department of Homeland Security.[43] In short, for government policymakers, there is little that cybersecurity does *not* cover.

Similarly, legal scholars define the concept expansively. Gus P. Coldebella and Brian M. White see cybersecurity as encompassing "criminality of all stripes, nation state and corporate espionage, and attack[s]," even while they decry term-creep in the concept.[44] Sean M. Condron, of the U.S. Army's Judge Advocate General's Legal Center and School,[45] defines

39. National Cyber Infrastructure Protection Act of 2010, S. 3538, 111th Cong. § 2(3) (2010), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-111s3538is/pdf/BILLS-111s3538is.pdf.

40. *Id.*

41. Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. § 3(9) (2010), *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bba-04b7f4cb0123.

42. Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. § 221(3) (2011), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr174ih/pdf/BILLS-112hr174ih.pdf.

43. *Id.* §§ 221(2), 224(e).

44. Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 235–36 (2010).

45. Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 403 (2007).

the problem as attacks on critical infrastructure by "terrorists, nation-states, terrorist sympathizers, and thrill seekers,"[46] where critical infrastructure comprises networked computer systems "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[47] Susan Brenner, in her Article classifying cybersecurity risks based on the actor's intent, defines cyberthreats as those "using computer technology to engage in activity that undermines a society's ability to maintain internal or external order."[48] Milton L. Mueller decries the fact that "the term *security* now encompasses a host of problems, perhaps too many to fit properly under one word."[49] However, he then proposes a governance-based approach to cybersecurity without offering a coherent definition of the term, and includes spam, phishing, and surveillance as representative threats.[50]

Even scholars who purportedly focus on narrower aspects of cybersecurity employ commodious definitions. Kelly Gable, who concentrates on cyberterrorism, defines it as "efforts by terrorists to use the Internet to hijack computer systems, bring down the international finance system, or commit analogous terrorist actions in cyberspace."[51] A 2001 report by Steven A. Hildreth of the Congressional Research Service describes cyberwarfare as "various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same."[52] Brenner defines cybercrime as "the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order."[53] Richard Clarke, former Special Advisor on Cybersecurity to President George W. Bush, and co-author Robert Knake even conceive of cybersecurity as encompassing

46. *Id.* at 404 (citing Michael A. Vatis, *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, INST. FOR SECURITY TECH. STUD. AT DARTMOUTH C., 1 (2001), http://www.ists.dartmouth.edu/docs /cyber_a1.pdf).

47. *Id.* at 406 (adopting definition from 42 U.S.C. § 5195c(e) (2006)).

48. Brenner, *supra* note 17, at 381.

49. MUELLER, *supra* note 27, at 159.

50. *Id.* at 165–79.

51. Gable, *supra* note 19, at 62.

52. STEVEN A. HILDRETH, CONG. RESEARCH SERV., RL3073, CYBERWARFARE, Summary (2001), *available at* http://www.fas.org/irp/crs/RL30735.pdf.

53. Brenner, *supra* note 17, at 386.

intellectual property theft.[54] These definitions of cybersecurity are vague, overbroad, and not helpful. Each attempt at framing the cybersecurity problem implicitly sets a standard for addressing the problem, for prioritizing it relative to competing concerns, and for measuring progress. Inaccurate cybersecurity definitions impede these efforts.

Conceptual failures—shortcomings in theoretical orientation—are largely to blame for what all commentators agree is an utter lack of success in improving cybersecurity.[55] Legal scholarship has thus far approached cybersecurity questions from within well-established, comfortable, yet poorly fitting models from criminal law, national security law, and military law. These doctrinal frameworks push scholars to concentrate upon the identity of actors behind a cyberthreat, and to determine their intent.[56] The problem is that the Internet's design makes attribution extremely difficult.[57] Tracing an attack to a given computer is challenging; deciphering who operated that computer during the attack is harder yet; and discerning motive can be nearly impossible.[58] The chief culprit, for most

54. CLARKE & KNAKE, *supra* note 23, at 236–37.

55. *See, e.g.*, NAT'L RESEARCH COUNCIL, TOWARD A SAFER AND MORE SECURE CYBERSPACE 9–10 (Seymour E. Goodman & Herbert S. Lin eds., 2007) ("After more than 15 years of reports pointing to an ominous threat, and in fact more than 15 years in which the threat has objectively grown, why is there not a national sense of urgency about cybersecurity? Why has action not been taken to close the gap between the nation's cybersecurity posture and the cyberthreat?").

56. *See, e.g.*, Brenner, *supra* note 17, at 438–40 (discussing the implications of the difficulty of discerning motivations for some cyberattacks); Dycus, *supra* note 22 (noting the difficulty of identifying the source of a cyberattack); Gable, *supra* note 19, at 105 (arguing for universal jurisdiction for cyberattacks based on the common motivations of "political, religious, or ideological causes").

57. *See, e.g.*, CLARKE & KNAKE, *supra* note 23, at 214–15, 248 (detailing the troubles that computer forensics experts have in tracing the sources of cyberattacks and the further problem that, even if forensics could trace an attack to a nation-state, the leaders could claim that an anonymous citizen carried it out); NAT'L RESEARCH COUNCIL, *supra* note 55, at 46, 49 (discussing how high-level cyberattackers could conceal their identities); Gable, *supra* note 19, at 100–02 (describing the technological difficulties of tracking a cyberattack over the Internet); Jensen, *supra* note 24 (explaining how the relative anonymity of IP addresses affords attackers, especially foreign governments, "plausible deniability").

58. Attribution must identify both the computer and the operator involved. *See, e.g.*, CLARKE & KNAKE, *supra* note 23, at 214–15 (explaining why simply knowing the computer network in which an attack originates is not sufficient to attribute the attack to a particular actor). Many security-compromised computers are part of botnets, which are "network[s] of comput-

scholars, is the lack of an authentication mechanism in the Internet's core TCP/IP protocols.[59] The Internet routes data in best-efforts fashion, regardless of who sent it.[60] Indeed, there is simply no way to verify a sender's identity under TCP/IP; functions such as authentication and error-checking are left to higher-level network layers and applications.[61] This default setting, which permits unattributed communication, is frequently exploited by malefactors—Internet traffic can be generated by botnets of suborned computers available for rent, or from computers specifically compromised for purposes of an attack.[62]

Recent cybersecurity incidents illustrate the problem. The cyberassault on Estonia during that country's conflict with Russia in May 2007 originated in part from computers located in Brazil and Vietnam.[63] The July 2009 denial of service attack against South Korea and the U.S., widely attributed to North

ers that have been forced to operate on the commands of an unauthorized remote user, usually without the knowledge of their owners or operators." *Id.* at 282. The malicious programs used to create botnets ("bots" or "robots") are extremely difficult to detect; hence, the actor may be unaware of the malicious manner in which her computer is actually functioning. BERNADETTE SCHELL & CLEMENS MARTIN, WEBSTER'S NEW WORLD HACKER DICTIONARY 42 (2006).

59. *See, e.g.*, Chris Chambers et al., *TCP/IP Security*, LINUXSECURITY.COM, § 3.2, http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html (last visited Nov. 7, 2011) ("The utter lack of authentication with IP packets is a general weakness with TCP/IP. Without authentication, there really is no guarantee that a packet comes from where its source field claims it comes from. This is . . . the major issue in IP security."). *See generally Request for Comments 1122: Requirements for Internet Hosts—Communication Layers*, INTERNET ENG. TASK FORCE (R. Braden ed., Oct. 1989), http://tools.ietf.org/pdf/rfc1122.pdf (defining Transmission Control Protocol [TCP] and Internet Protocol [IP]).

60. *E.g.*, JEAN WALRAND & SHYAM PAREKH, COMMUNICATION NETWORKS: A CONCISE INTRODUCTION 18–19 (2010).

61. *See, e.g.*, 1 INFORMATION SECURITY MANAGEMENT HANDBOOK 114 (Harold F. Tipton & Micki Krause eds., 5th ed. 2004) (describing higher-level network layers and applications used to make Internet connections more secure).

62. NAT'L RESEARCH COUNCIL, *supra* note 55, at 115–16; Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1058–59, 1067 (2011). *See generally* Info. Warfare Monitor & Shadowserver Found., *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, SCRIBD (Apr. 6, 2010) [hereinafter *Shadows in the Cloud*], http://www.shadows-in-the-cloud.net (documenting GhostNet cyberespionage malware).

63. SUSAN W. BRENNER, CYBERTHREATS 133–34 (2009); Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 27, 2007, at A1.

Korea,[64] was launched from computers in Austria, Georgia, Germany, and even South Korea and America.[65] In both cases, initial judgments that a State (Russia or North Korea) was responsible dissolved into uncertainty in the face of mixed evidence. Attribution is thus an intolerably hard problem for conventional legal approaches. Worse, it is one that flows directly from the architecture of the Internet.[66]

Unsurprisingly, the predominant answer to this perceived shortcoming is to retrofit attribution capabilities into the core of the Internet. Clarke and Knake want to move to new networks where "the user's authenticated identity could be embedded in each packet."[67] Jeffrey A. Hunker too believes that the "existing Internet architecture is fundamentally insecure."[68] He seeks to replace the Internet with a network that allows "different governments to have different rules," where governments "protect their citizens on the Internet the same way they protect them" in other media.[69] Former Director of National Intelligence Mike McConnell argues "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment . . . more manageable."[70] Former CIA Director Michael V. Hayden proposes creating a new, "hardened enterprise structure" for the Internet that

64. *Pentagon Official: North Korea Behind Week of Cyber Attacks*, FOXNEWS.COM (July 9, 2009), http://www.foxnews.com/story/0,2933,530781,00.html. *But see* Lolita C. Baldor, *US Largely Ruling Out North Korea in 2009 Cyber Attacks*, USATODAY (July 6, 2010, 11:45 AM), http://www.usatoday.com/tech/news/computersecurity/2010-07-06-nkorea-cyber-attacks_N.htm (stating that U.S. government experts had "largely ruled out" North Korea as the source of the attacks).

65. D.J. Walker-Morgan, *DDoS Attacks with Zombie Computers—'North Korea's Powerful Hacker Army'?*, THE H SECURITY (July 10, 2009, 1:49 PM), http://www.h-online.com/security/news/item/DDoS-attacks-with-zombie-computers-North-Korea-s-powerful-hacker-army-742435.html.

66. *See, e.g.*, CLARKE & KNAKE, *supra* note 23, at 214–15 (discussing how the structure of the Internet makes attribution of cyberattacks difficult); Gable, *supra* note 19, at 84 (stating "[a]s a result of the inherent insecurity of the TCP/IP Protocol, . . . it is remarkably easy to attack any network that is based on that protocol," including the Internet).

67. CLARKE & KNAKE, *supra* note 23, at 275.

68. Hunker, *supra* note 14, at 207.

69. *Id.* (quoting Raj Jain, *Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation*, WASH. U. ST. LOUIS, http://www.cse.wustl.edu/~jain/papers/ftp/gina.pdf (last visited Nov. 7, 2011)).

70. Mike McConnell, *To Win the Cyber-War, Look to the Cold War*, WASH. POST, Feb. 28, 2010, at B1.

would embed identification capabilities into its architecture.[71] Stuart Biegel states that "code-based adjustments in Internet architecture . . . can go a long way toward countering cyberterrorism."[72] Greater attribution enables the traditional practice of deterrence, along with traditional distinctions among criminals, terrorists, soldiers, and spies.[73] By building strong attribution into networking protocols, lawyers (and their governments) can apply time-tested ways of thinking and reacting to threats online. However, trying to redesign the architecture of the Internet as a solution has at least three critical shortcomings: difficult implementation, unintended consequences, and loss of generativity.

A. IMPLEMENTATION CHALLENGES AND NETWORK EFFECTS

First, effecting a change to core Internet protocols would be extremely difficult. The Internet's success and ubiquity rest largely on the role of TCP/IP as the lingua franca for information exchange.[74] Network effects drove adoption: any device using TCP/IP that attaches to the Internet can immediately communicate with every other point on the Net.[75] Changing TCP/IP would require altering each of those devices' networking stacks—no small task when there are over 845 million hosts directly connected to the Internet.[76] Moreover, key stake-

71. Aliya Sternstein, *Former CIA Director: Build a New Internet to Improve Cybersecurity*, NEXTGOV (July 6, 2011), http://www.nextgov.com/nextgov/ng_20110706_1137.php?oref=topnews.

72. STUART BIEGEL, BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 256–57 (2003).

73. *See, e.g.*, NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 17, at 113–18 (discussing how more accurate attribution on the Internet can foster accountability for cyberattacks); Brenner, *supra* note 17, at 404, 438 (discussing how attribution problems make it difficult to differentiate between crime, terrorism, and war during cyberattacks).

74. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 60, 67–100 (2008) (explaining that "if the Internet had been designed with security as its centerpiece, it would never have achieved the kind of success it was enjoying" and describing the "generative pattern" of the Internet, which is essentially the idea that the Internet's architecture fosters innovation).

75. *See* STAN J. LIEBOWITZ, RE-THINKING THE NETWORK ECONOMY 13–14 (2002) (defining network effects as the increased benefit in using a network that comes with the rise in the number of other people using the network).

76. *Internet Domain Survey*, INTERNET SYS. CONSORTIUM (July 2011), http://ftp.isc.org/www/survey/reports/current/ (reporting 849,869,781 hosts advertised on the Domain Name System (DNS) as of July 2011). For methodology, see *The Domain Survey*, INTERNET SYS. CONSORTIUM, http://ftp.isc.org/www/survey/reports/current/survey.html (last visited Nov. 7, 2011).

holders such as Internet Service Providers (ISPs), operating system vendors (particularly Microsoft), the Internet Engineering Task Force (IETF), and possibly even the Internet Corporation for Assigned Names and Numbers (ICANN) would have to come to consensus, not only about the need for such a change, but also about the method to accomplish it.

Consider two illustrative examples: Internet Protocol version 6 (IPv6)[77] and spam. First, network administrators have encountered significant delays in migrating from IPv4 to IPv6.[78] This change should be straightforward. IPv6 is compatible with IPv4, at least with certain transition mechanisms,[79] and has few controversial features (unlike attribution).[80] Furthermore, everyone acknowledges the shift's necessity[81]—the Internet Assigned Numbers Authority (IANA) distributed the remaining IPv4 addresses to the five regional Internet registries (RIRs) in February 2011.[82] One RIR began a strict IPv4 address delegation policy in April 2011 to postpone IPv4 ex-

77. *See generally* S. Deering & R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification* (Dec. 1998), http://www.rfc-editor.org/rfc/pdfrfc/rfc2460.txt.pdf (discussing the technical details of IPv6); *IPv6*, MICROSOFT, http://technet.microsoft.com/en-us/network/bb530961 (last visited Nov. 7, 2011) (introducing IPv6 and explaining its utility).

78. *See* Mónica Domingues and Carlos Friaças, *Is Global IPv6 Deployment on Track?*, 17 INTERNET RES. 505, 506 (2007) (acknowledging the slow adoption of IPv6).

79. *See* Carolyn Duffy Marsan, *Biggest Mistake for IPv6: It's Not Backwards Compatible, Developers Admit*, NETWORK WORLD (Mar. 25, 2009, 8:23 AM), http://www.networkworld.com/news/2009/032509-ipv6-mistake.html (noting that, although IPv6 is not backwards compatible on its own, the use of transition mechanisms can integrate IPv6 with IPv4); *see also* Carolyn Duffy Marsan, *'IPv6 Brokenness' Problem Appears Fixed*, NETWORK WORLD (July 27, 2011, 3:08 PM), http://www.networkworld.com/news/2011/072711-ipv6-brokenness.html.

80. *See* Deering & Hinden, *supra* note 77.

81. *See, e.g.*, News Release, The Internet Corp. for Assigned Names and Numbers (ICANN), Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied 1 (Feb. 3, 2011), http://www.icann.org/en/news/releases/release-03feb11-en.pdf ("[T]he future expansion of the Internet is now dependant on the successful global deployment of the next generation of Internet protocol, called IPv6.").

82. *See, e.g.*, *id.*; Geoff Huston, *IPv4 Address Report*, POTAROO, http://www.potaroo.net/tools/ipv4/index.html (last visited Nov. 7, 2011) (continuously calculating projected IPv4 address exhaustion); Antone Gonsalves, *IP Addresses Predicted to be Exhausted In 2011*, INFORMATIONWEEK (July 27, 2010), http://www.informationweek.com/news/software/showArticle.jhtml?articleID=226300002.

haustion.[83] And the remaining four RIRs are expected to exhaust their pools of IPv4 addresses within the next three years.[84] Yet IPv6 deployment has been quite slow, to the concern of observers such as the OECD.[85] By early 2010, only 5.5% of Internet-connected networks could handle IPv6; only 0.25% of Internet users had IPv6 connectivity; and only 0.16% of the top million sites on the Web offered IPv6 support.[86] It is difficult to make even minor changes to ubiquitous standards.[87]

Next, think about spam. Everyone hates it and there is widespread consensus about which e-mail messages qualify as spam.[88] Moreover, spam creates a considerable, expensive burden for ISPs: it comprises nearly eighty percent of e-mail traffic.[89] Like cybersecurity, spam results from an attribution problem: the protocol for e-mail transfer, Simple Mail Transfer Protocol (SMTP), does not verify a sender's identity.[90] Thus, one can readily falsify a message's source. Re-engineering SMTP to implement authentication was rejected as too difficult to deploy, given the installed base of e-mail clients and servers.[91] Various messaging-related entities—Microsoft, Yahoo!, the IETF—sought to craft add-on components to deal with attribution.[92]

83. *See Policies for IPv4 Address Space Management in the Asia Pacific Region*, ASIA-PAC. NETWORK INFO. CTR. (May 9, 2011), http://www.apnic.net/policy/add-manage-policy.

84. Huston, *supra* note 82.

85. *See* ORG. FOR ECON. CO-OPERATION & DEV., INTERNET ADDRESSING: MEASURING DEPLOYMENT OF IPV6 40–42 (2010), *available at* http://www.oecd.org/dataoecd/48/51/44953210.pdf (noting the critical situation of IPv4 exhaustion and urging for governmental and international cooperation in transitioning to IPv6).

86. *Id.* at 4–5.

87. *See* LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE 225–28 (2009).

88. *See* DEREK E. BAMBAUER ET AL., INT'L TELECOMM. UNION, A COMPARATIVE ANALYSIS OF SPAM LAWS: THE QUEST FOR MODEL LAW 26–27 (2005), *available at* http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf.

89. Mathew J. Schwartz, *Spam Plummets to 2009 Levels*, INFO.WEEK (Jan. 26, 2011, 1:38 PM), http://www.informationweek.com/news/security/management/229100295?cid=RSSfeed_IWK_News.

90. *See* Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. 5, ¶ 14 (2005), http://www.vjolt.net/vol10/issue2/v10i2_a5-Bambauer.pdf.

91. *Id.* ¶ 17 & nn.52–53.

92. *Id.* ¶¶ 34–44.

Efforts to combine the resulting schemes failed,[93] and anti-spam technologies remain fragmented. Network effects, and competition to define how attribution would work, defeated protocol changes that might have greatly reduced spam.[94]

As spam and IPv6 demonstrate, even widespread consensus on a problem created by shortcomings in core Internet protocols, and on the need for a technological solution, may not result in a fix.

B. ATTRIBUTION'S UNINTENDED CONSEQUENCES

The second shortcoming to re-designing the architecture of the Internet is that attribution is not an unalloyed good and would have unintended consequences. An authenticated Internet would be one with both fewer viruses and less dissent. It would change who can communicate, how free they feel to do so, and the ways in which that information exchange is governed. China, for example, has moved steadily to force users to employ their real names online.[95] Indeed, part of China's push to deploy IPv6 is the country's desire to increase attribution and accountability online.[96] With a sufficient number of IP addresses, China could allocate a single permanent address to each Internet-connected device, and seek to trace data to that source. Enhancing attribution means facing hard tradeoffs: not only between values such as security and free expression, but between different users. American users might benefit from authentication, since their ability to engage in free expression (including anonymously) is protected through law,[97] while Chinese users might suffer, since their government actively impedes communication on certain topics.[98] China's government itself

93. Jim Wagner, *IETF Shutters E-mail Working Group*, INTERNETNEWS.COM (Sept. 22, 2004), http://www.internetnews.com/bus-news/article.php/3411461/IETF+Shutters+Email+Working+Group.htm.

94. *See* Bambauer, *supra* note 90, ¶¶ 43–47.

95. *See* ACCESS CONTROLLED: THE SHAPING OF POWER RIGHTS, AND RULE IN CYBERSPACE 464–65 (Ronald Deibert et al. eds., 2010) [hereinafter ACCESS CONTROLLED]; Peter Foster, *China to Force Internet Users to Register Real Names*, The TELEGRAPH (May 5, 2010, 12:40 PM), http://www.telegraph.co.uk/news/worldnews/asia/china/7681709/China-to-force-internet-users-to-register-real-names.html.

96. Rana Foroohar & Melinda Liu, *It's China's World We're Just Living in It*, NEWSWEEK, Mar. 22, 2010, at 36, 38.

97. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995).

98. *See* ACCESS CONTROLLED, *supra* note 95, at 449–87 (documenting China's employment of sophisticated online filtering and surveillance systems to suppress free speech).

might be conflicted: attribution could augment its internal security controls, but weaken its capabilities to mount a deniable cyberattack. Embedding attribution in the Internet's core is not merely a technical change: it is a choice among competing normative models of how the network should function, and who should benefit.[99]

C. FORFEITING GENERATIVITY

The third shortcoming is that greater security through code may damage the Internet's generativity. It is likely to alter the Internet's power as a platform for technological innovation. Jonathan Zittrain, Yochai Benkler, David G. Post, Tim Wu, Barbara van Schewick, and other cyberscholars make the powerful case that the Internet's value as a communications platform comes from its open, end-to-end architecture.[100] No one need ask permission before creating and deploying a new application.[101] Changing this design by replacing automatic routing that is identity-agnostic with authenticated communication risks destroying the Net's generativity. Attribution requires, at minimum, that data carry an identifying signal, and that routing devices be designed to inspect, and make decisions based upon, that information. Even proponents concede this would slow routing.[102] More importantly, it changes the Internet's default behavior: anonymous information would go from being the norm to being suspect. A permission-based Internet could well suffer the same shortcomings as the circuit-switched telephone network did in spurring innovation.[103] When gatekeepers can veto changes by withholding assent—such as AT&T's objections to network-attached equipment as innocuous

99. *Cf.* MUELLER, *supra* note 27, at 180–82 (noting that "by creating a system of 'identification' on the Internet, we are answering fundamental questions about the nature and scope of government").

100. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006); DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE (2009); BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (2010); ZITTRAIN, *supra* note 74 *passim*; J.H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYS. 277 (1984); Tim Wu & Christopher Yoo, *Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate*, 59 FED. COMM. L.J. 575 (2007).

101. *See* Zittrain, *supra* note 29.

102. CLARKE & KNAKE, *supra* note 23, at 161.

103. *See* Wu & Yoo, *supra* note 100, at 577–78, 581–83.

as a rubber mouthpiece designed to make conversations more private[104]—they often do, either out of caution or self-interest.

Changing the Internet's architecture to enable attribution is attractive to scholars who need this capability to employ standard doctrinal models for cybersecurity. However, they fail to consider the countervailing risks of deployment challenges, unintended consequences, and loss of generativity. Their proposals to save the Internet could destroy it.

Wide-ranging governmental policies and scholarly efforts to cram cybersecurity into existing models of thinking reflect not only comfort with the familiar, but a response to widespread near-panic over a looming cyber-apocalypse.[105] The next Part examines these fears and why they are likely overblown.

II. APOCALYPSE NOW?

> Within a quarter of an hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed in New York, Oakland, Washington, and Los Angeles. Freight trains have derailed outside major junctions and marshaling yards on four major railroads. Aircraft are literally falling out of the sky as a result of midair collisions across the country. Pipelines carrying natural gas to the Northeast have exploded, leaving millions in the cold. The financial system has frozen solid because of terabytes of information at data centers being wiped out.[106]

A. RAGNAROK

Cyberspace is falling—if not now, then soon. Policymakers are fearful. The National Research Council of the National Academies warns of a "digital Pearl Harbor."[107] Former counterterrorism coordinator Richard Clarke describes the risk of "a massive cyberattack on civilian infrastructure that smacks down power grids for weeks, halts trains, grounds aircraft, explodes pipelines, and sets fires to refineries."[108] Senator Harry

104. *See* Hush-A-Phone v. United States, 238 F.2d 266, 267–68 (D.C. Cir. 1956) (noting that intervenors, including AT&T, filed tariffs with the FCC forbidding the attachment of petitioner's device to intervenors' telephones, even though the device "[did] not impair any of the facilities of the telephone companies").

105. *See* Jonathan Zittrain, *The Fourth Quadrant*, 78 FORDHAM L. REV. 2767, 2776 (2010) ("[T]here is rising panic over the situation.").

106. CLARKE & KNAKE, *supra* note 23, at 67.

107. NAT'L RESEARCH COUNCIL, *supra* note 55, at 50.

108. CLARKE & KNAKE, *supra* note 23, at 260.

M. Reid stated that "Cyber attack could, for example, bring down our nation's air traffic control system in a matter of seconds";[109] Senator Joseph I. Lieberman agreed that the "future security of the American way of life depends on passage of comprehensive cyber security legislation."[110]

Scholars and technologists also view the situation in catastrophic terms. Kelly Gable writes of a "cyber-apocalypse," where "Al Qaeda replace[s] the White House website with a message that they have hacked into and shut down [cities'] major power grids to cripple the U.S. economy . . . ."[111] The chief security officer for Oracle warned of terrorist attacks on critical infrastructure, saying, "'[M]ove the control rods in and out of the reactor? There's an app for that.'"[112] Former Direct of National Intelligence Mike McConnell states that a large-scale cyberattack on the U.S. could have global economic effects on "'an order of magnitude surpassing' the [terrorist] attacks of September 11 [2001]."[113] Analyst Franz-Stefan Gady writes of the risk that a botnet based in Africa could "bring down the world's top 10 leading economies with just a few strokes."[114] President Obama's Cyberspace Policy Review summarizes the consensus viewpoint, describing the lack of cybersecurity as "[o]ne of the most serious economic and national security threats of the 21st Century for the United States."[115]

These descriptions are alarmist, and inaccurate.[116] Overestimating risks from the Internet, hackers, and software vulner-

109. *Senate Democrats Introduce Legislation Calling for New Safeguards for National Security, American Economy Against Cyber Attack*, U.S. SENATE DEMOCRATS (Jan. 26, 2011, 8:00 AM), http://democrats.senate.gov/2011/01/26/senate-democrats-introduce-legislation-calling-for-new-safeguards-for-national-security-american-economy-against-cyber-attack/.

110. *Id.*

111. Gable, *supra* note 19, at 59; *see also* Dycus, *supra* note 22, at 156 ("The very future of the Republic rests on . . . protect[ing] ourselves from enemies armed with cyber weapons . . . .").

112. Elinor Mills, *Experts Warn of Catastrophe from Cyberattacks*, CNET NEWS (Feb. 23, 2010, 6:35 PM), http://news.cnet.com/8301-27080_3-10458759-245.html.

113. Max Fisher, *Fmr. Intelligence Director: New Cyberattack May Be Worse than 9/11*, THE ATLANTIC (Sept. 30, 2010, 2:28 PM), http://www.theatlantic.com/politics/archive/2010/09/fmr-intelligence-director-new-cyberattack-may-be-worse-than-9-11/63849/.

114. Franz-Stefan Gady, *Africa's Cyber WMD*, FOREIGN POL'Y (Mar. 24, 2010), http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd?page=full.

115. CYBERSPACE POLICY REVIEW, *supra* note 35, at 1.

116. *See* Evgeny Morozov, *Cyber-Scare*, BOS. REV., July/Aug. 2009, at 17, *available at* http://www.bostonreview.net/BR34.4/morozov.php. Compare the

abilities is common—Paul Ohm refers to the "myth of the superuser."[117] They are also not accidental. Increasing the attention and funding devoted to cybersecurity will benefit important interests, from the software security community,[118] to agencies like the Department of Homeland Security,[119] to policy think tanks.[120] Regulatory competition among federal government agencies has been a recurring theme in Internet security efforts.[121] Downplaying risks is not an effective way to gain authority (and a budget) to combat them. Some cybersecurity commentators also have potential conflicts of interest. Richard Clarke now operates a consulting firm that offers cybersecurity risk consulting.[122] Stewart A. Baker, former Assistance Secretary for Policy at DHS, who worries about "freezing in the dark because of cyberweapons,"[123] is a partner at the law firm of Steptoe & Johnson, with a practice covering national security and technology.[124] Mike McConnell rejoined the consulting firm Booz Allen Hamilton as leader of its Intelligence business; the firm recently received $34 million in government contracts for cybersecurity.[125] This is not to suggest bad faith on the part of

quotes above, *supra* text accompanying notes 107–15, with dialogue from the film *Live Free or Die Hard*, where a character describes "a three-step systematic attack on the entire national infrastructure. . . . [T]hat's why they call it a fire sale—because everything must go." LIVE FREE OR DIE HARD (20th Century Fox 2007).

117. *See* Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1333–40, 1342–48 (2008).

118. *See generally* JOHN VIEGA, THE MYTHS OF SECURITY: WHAT THE COMPUTER SECURITY INDUSTRY DOESN'T WANT YOU TO KNOW (2009) (discussing the poor state of cybersecurity and suggesting various changes to improve it).

119. Ben Bain, *DHS Would Be Cyber Power Center Under Lieberman/Collins Proposal*, FED. COMPUTER WK. (June 10, 2010), http://fcw.com/articles/2010/06/10/web-lieberman-collins-carper.aspx.

120. *See, e.g.*, *Commission on Cybersecurity for the 44th Presidency*, CTR. FOR STRATEGIC & INT'L STUD., http://csis.org/program/commission-cybersecurity-44th-presidency (last visited Nov. 7, 2011).

121. *See* Coldebella & White, *supra* note 44, at 233 (identifying the problem of bureaucratic leadership and accountability as a "thorny" issue in federal cybersecurity).

122. *Partners*, GOOD HARBOR CONSULTING, http://www.goodharbor.net/team/index.php (last visited Oct. 28, 2011) ("Good Harbor is led by Richard A. Clarke . . . .").

123. Stewart Baker, *Cyberscam Hits OECD*, THE VOLOKH CONSPIRACY (Jan. 17, 2011, 9:20 PM), http://volokh.com/2011/01/17/cyberscam-hits-oecd/.

124. *Stewart A. Baker*, STEPTOE & JOHNSON, http://www.steptoe.com/professionals-762.html (last visited Nov. 7, 2011).

125. *John M. (Mike) McConnell: Executive Vice President*, BOOZ ALLEN HAMILTON (Sept. 2010), http://www.boozallen.com/about/leadership/executive-leadership/McConnell; Ryan Singel, *Cyberwar Doomsayer Lands $34 Million in*

these groups or individuals, but rather to state that they have incentives to convey a compelling image of dramatic cybersecurity threats.

Even fakery may generate overblown claims. Guerrilla marketing firm The Brainstormclub created a viral video ostensibly showing hackers taking control of the lighting in two skyscrapers to play a colossal game of Space Invaders.[126] A McAfee Avert Labs researcher wrote that "[p]erhaps the first demo was just for fun, but the others will have less juvenile goals . . . . An attack can involve nationwide damage . . . ."[127] The video, though, was fiction. Although computers created the giant Space Invaders match, they were Brainstormclub's graphic production ones, not the Supervisory Control and Data Acquisition (SCADA) systems in the buildings.[128] Nonetheless, McAfee's blogger asserted, "fake or not, the video confirms that hackers and cybercriminals have got their eyes on SCADA networks."[129] Perhaps this is because "McAfee's recent acquisition of Solidcore will help [its] customers" secure SCADA systems against cyberattack, or at least rogue marketers.[130]

Scholars and commentators describe cyberthreats in dramatic, even cataclysmic, terms. These fears have generated a regulatory stampede, though proposals to date have not only failed to define the extent of the problem, but also to craft a coherent solution.

B. REACTION

Florid descriptions of imminent, catastrophic risk in cyberspace have produced a rush to regulate cybersecurity.[131] Indeed, in the summer of 2010, an election year, over twenty cy-

Government Cyberwar Contracts, WIRED (Apr. 13, 2010, 6:04 PM), http://www.wired.com/threatlevel/2010/04/booz-allen/.

126. *Urban Hack Attack*, BRAINSTORMCLUB, http://brainstormclub.net/project/urban_hack_attack/ (last visited Nov. 7, 2011).

127. Francois Paget, *Urban "Attack" on Infrastructure*, MCAFEE (May 22, 2009, 6:59 AM), http://blogs.mcafee.com/mcafee-labs/urban-attack-on-infrastructure.

128. *See* Kevin Poulsen, *Viral Video Hoax, or Proof of Impending Cyber Apocalypse?*, WIRED (May 26, 2009, 7:08 PM), http://www.wired.com/threatlevel/2009/05/viral-video-hoax-or-proof-of-impending-cyber-apocalypse/.

129. Paget, *supra* note 127.

130. *Id.*

131. *See generally* David W. Opderbeck, *Cybersecurity and Executive Power* (2011) (Seton Hall U. Sch. of Law Legal Studies Research Paper Series No. 1788333), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1788333 (follow "One-Click Download" hyperlink to download PDF document) (describing recent cybersecurity legislation).

bersecurity bills were pending in Congress.[132] Regulatory proposals to prevent the fall of cyberspace tend to suffer similar shortcomings. They fail to describe precisely the cybersecurity problem which is to be solved, and thereby put forward measures that are either too small or too great in coverage. Purported reforms are often parochial: they focus on shuffling authority for security among government agencies, or between branches of government. And some proposals are simply stupid: Stewart Baker believes that users should have to obtain an "Internet driver's license" before being permitted online,[133] and Jeffrey Carr, unintentionally copying China's approach,[134] seeks to compel ISPs to verify their customers' real identities.[135] This Section reviews recent cybersecurity efforts, and their failings.

To date, proposals to use law to improve cybersecurity have been strikingly minimalist (particularly when compared to the apocalyptic rhetoric used to describe the problem), or, on occasion, incredibly broad. In the minimalist camp, President Obama's administration has advanced policies that are highly deferential in regulating entities such as Internet service providers, equipment manufacturers, and utility operators. Obama's sixty-day Cybersecurity Policy Review emphasizes public-private partnerships, information sharing, financial incentives through procurement strategy and tax benefits, and investment in research.[136] Regulatory mandates, such as requiring private entities to share information with government cybersecurity officials, are expressly a "last resort."[137] Clarke and Knake note that Obama "went out of his way to take regu-

132. Gautham Nagesh, *Senators Debate Terms of Cybersecurity Overhaul*, THE HILL (June 29, 2010, 10:33 AM), http://thehill.com/blogs/hillicon-valley/technology/106119-senators-debate-terms-of-cybersecurity-overhaul.

133. John Markoff, *Taking the Mystery Out of Web Anonymity*, N.Y. TIMES, July 4, 2010, at WK3.

134. Alex Fayette, *Chinese Plans to Deanonymize the Internet*, OPENNET INITIATIVE (July 22, 2010), http://opennet.net/blog/2010/07/chinese-plans-to-deanonymize-the-internet.

135. Seymour Hersh, *The Online Threat*, THE NEW YORKER, Nov. 1, 2010, at 44, 55. Carr's proposal is almost certainly unconstitutional. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.").

136. CYBERSPACE POLICY REVIEW, *supra* note 35, at iii–v.

137. *Id.* at 26.

lation off the table."[138] For example, Howard Schmidt, the administration's coordinator for cybersecurity, endorsed mandatory encryption for Internet communication by firms in the electrical and power industries.[139] However, President Obama refused to support Schmidt's recommendation, citing financial and logistical costs for affected corporations.[140] Even the administration's identity management initiative, which addresses attribution problems widely viewed as central to cybersecurity, is a voluntary program that contemplates multiple vendors and optional adoption.[141] Many congressional proposals have been equally small-scale,[142] focusing on which executive agency should lead cybersecurity efforts (typically devolving into a contest between the Department of Defense and the Department of Homeland Security),[143] establishing a consortium to train state and local first responders,[144] or setting priorities for research and development funding.[145] In short, where cybersecurity is concerned, the Obama administration and Congress are usually chary of legal mandates. (Contrast this reluctance, though, with the administration's willingness to regulate the design of Internet applications to enable eavesdropping,[146] and to ensure that ISPs retain data to aid law enforcement.[147]).

138. CLARKE & KNAKE, *supra* note 23, at 118.

139. Hersh, *supra* note 135, at 51.

140. *Id.*

141. THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE 11–12 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf; *see* James Sterngold, *Say Goodbye to All Those Passwords*, BUSINESSWEEK (Jan. 27, 2011, 5:00 PM), http://www.businessweek.com/magazine/content/11_06/b4214036537462.htm.

142. Coldebella & White, *supra* note 44, at 242.

143. *Compare, e.g.*, Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. § 222(a)(1) (2011), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr174ih/pdf/BILLS-112hr174ih.pdf (establishing "an Office of Cybersecurity and Communications" in the Department of Homeland Security), *with* National Cyber Infrastructure Protection Act of 2010, S.3538, 111th Cong. § 102(a) (2010), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-111s3538is/pdf/BILLS-111s3538is.pdf (establishing a "National Cyber Center" in the Department of Defense).

144. Cyber Security Domestic Preparedness Act, H.R. 4507, 111th Cong. § 226(b) (2010), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-111hr4507ih/pdf/BILLS-111hr4507ih.pdf.

145. Cybersecurity Enhancement Act of 2010, H.R. 4061, 111th Cong. §§ 101–113 (2010), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-111hr4061eh/pdf/BILLS-111hr4061eh.pdf (as passed by House, Feb. 4, 2010).

146. *See* Charlie Savage, *U.S. Is Working to Ease Wiretaps on the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1.

147. Jaikumar Vijayun, *DOJ Seeks Mandatory Data Retention Require-*

Minimalist approaches contemplate a minor role for government in cybersecurity, with considerable deference to private sector efforts and standards. This reticence is in tension with apocalyptic views of cyberthreats, as threats to national well-being typically involve significant government mandates. (The federal takeover of airport security in the wake of the terrorist attacks of September 11, 2001 is but one example.)[148] However, deference is widely favored. Gregory T. Nojeim, senior counsel for the Center for Democracy & Technology, who worries about civil liberties, argues that "[c]ybersecurity solutions that favor industry standards over government technology mandates will enhance security more efficiently and flexibly than those that do not."[149] Coldebella and White state that "owners of critical infrastructure have had the incentive to develop cybersecurity measures that are suited to their businesses," and thus any "centrally planned, one-size-fits-all regulatory scheme would almost certainly eliminate useful, industry-developed security measures and replace them with an ill-fitting, nondynamic slate of requirements."[150] There is a persistent reluctance to second-guess private sector cybersecurity decisions.

The proposed legislation garnering the most attention, however, is the infamous "kill switch" bill, which demonstrates cybersecurity law at its most grandiose. Senators Joseph Lieberman and Susan Collins introduced a wide-ranging bill that would increase funding for implementing security measures, bolster information sharing between the public and private sectors, create security standards for federal agencies, and—most controversially—confer broad emergency powers on the U.S. President to protect critical infrastructure.[151] The legislation would enable the President, when confronted with a cyber-emergency, to compel owners and operators of critical infra-

ment for ISPs, COMPUTERWORLD (Jan. 25, 2011, 8:15 PM), http://www.computerworld.com/s/article/9206379/DOJ_seeks_mandatory_data_retention_requirement_for_ISPs.

148. Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

149. Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 NAT'L SECURITY L. & POL'Y 119, 120 (2010).

150. Coldebella & White, *supra* note 44, at 241.

151. *See* Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. §§ 102(a), 246, 249(a) (2010), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-111s3480is/pdf/BILLS-111s3480is.pdf; *see also* Declan McCullagh, *Internet 'Kill Switch' Bill Will Return*, CNET NEWS (Jan. 24, 2011, 4:00 AM), http://news.cnet.com/8301-31921_3-20029282-281.html?tag=topStories1.

structure to implement emergency plans, including stopping data flow.[152] The bill received widespread criticism,[153] particularly after the government of Egypt ordered that country's major ISPs to cease routing data during anti-government protests in early 2011.[154] The underlying concept of the legislation—to allow America to "pull up the drawbridge" in case of a cyberattack—is one supported by commentators such as Clarke and Knake.[155] It plainly involves substantial augmentation of the government's control over private Internet infrastructure, although proponents contend the President has similar authority under the Communications Act of 1934.[156] The "kill switch" legislation runs counter to the trend of minimalist proposals for legal regulation of cybersecurity, which accounts in part for the heated opposition to the bill.[157]

The Lieberman-Collins bill, even if passed and signed into law, is unlikely to advance cybersecurity much, for three reasons. First, the bill is redundant: it is inconceivable that a network that was the source or conduit of cyberattacks would refuse to deal with the problem, or to cooperate with government efforts to do so.[158] Any provider sufficiently removed from American suasive pressures would likely also be immune from legal enforcement. Second, disconnecting networks is as likely to worsen the effects of a cybersecurity problem as to ameliorate them. Shutting down ISPs burdens legitimate uses at the same time it counteracts illegitimate ones. From an information perspective, reducing connectivity decreases authorized access to information, while also cutting the number of targets

152. S. 3480 § 249(a).

153. *ACLU Protests "Internet Kill Switch"*, KTAR.COM (Aug. 12, 2010), http://ktar.com/?nid=6&sid=1323951; David Kravets, *Internet "Kill Switch" Legislation Back in Play*, WIRED (Jan. 28, 2011, 6:09 PM), http://www.wired.com/threatlevel/2011/01/kill-switch-legislation/; *Statement on Lieberman-Collins-Carper Cybersecurity Bill*, CENTER FOR DEMOCRACY & TECH. (June 10, 2010), http://www.cdt.org/pr_statement/statement-lieberman-collins-carper-cybersecurity-bill.

154. David Zax, *Could Egypt Happen Here? Obama's Internet "Kill Switch"*, FAST COMPANY (Jan. 28, 2011), http://www.fastcompany.com/1721753/egypt-internet-kill-switch.

155. CLARKE & KNAKE, *supra* note 23, at 216.

156. *See* 47 U.S.C. § 606(c) (2006).

157. *See, e.g.*, Declan McCullagh, *Internet 'Kill Switch' Bill Gets a Makeover*, CNET NEWS (Feb. 18, 2011, 6:27 PM), http://news.cnet.com/8301-31921_3-20033717-281.html (describing ACLU opposition).

158. *Cf.* Ben Rooney, *Amazon's WikiLeaks Response Threatens Cloud Computing*, WALL ST. J. BLOG (Dec. 13, 2010), http://blogs.wsj.com/tech-europe/2010/12/13/amazons-wikileaks-response-threatens-cloud-computing/.

for an attacker. Third, if the model for disconnection follows Clark and Knake's "drawbridge" metaphor, where the key to mitigating an attack is to break contact with the wider Internet, then the kill switch will fail. Any serious cyberthreat would be launched from networks within the U.S. as well as (or instead of) outside it. Indeed, the cyberattacks against South Korea emanated in part from computers within that country.[159] The Stuxnet cyberweapon was introduced into Iran's computers from within that state.[160] Even Clarke and Knake admit that attacks would be launched from domestic networks as well as foreign ones.[161] It is useless to raise the drawbridge when the attackers are inside the castle. Thus, legal efforts to date, whether cautious or outsized, hold little promise of increasing cybersecurity.

Joint public-private efforts to date have focused primarily on encouraging private sector entities to increase their security, and to share data with the federal government. There is consensus, though, that information sharing has noticeably failed.[162] Owners of critical infrastructure have been reluctant to share information on intrusions and other cyberthreats. Explanations for this unwillingness include "fear [of] enforcement actions by regulators, suits by plaintiffs' lawyers, and criticism associated with public disclosure of security failures,"[163] along with concerns about censure from civil liberties advocates.[164] (The latter worry is entirely plausible; Nojeim argues that routine information sharing between providers and the government would be unlawful.)[165] Commentators have suggested remedying the shortcomings of suasive, norms-based models of information exchange by reshaping incentives through legislation. Thus, Coldebella and White suggest using law to eradicate the "structural disincentives" that, in their view, impede sharing vulnerability and incident data with other industry entities and with the government.[166] It is not clear, however, why the

159. *See supra* note 65 and accompanying text.

160. John Markoff, *Malware Aimed at Iran Hit Five Sites, Report Says*, N.Y. TIMES, Feb. 13, 2011, at A15.

161. *See* CLARKE & KNAKE, *supra* note 23, at 209.

162. Nojeim, *supra* note 149, at 126.

163. Coldebella & White, *supra* note 44, at 237.

164. *See, e.g.*, Nojeim, *supra* note 149, at 126.

165. *Id.*

166. Coldebella & White, *supra* note 44, at 236–37.

multiple existing protections for confidential reporting by the private sector to government actors are inadequate.[167]

Both government and private sector cybersecurity proposals typically involve using code to fight code. For example, the Department of Homeland Security has moved to implement its Einstein 3 program, which will monitor the networks of critical infrastructure operators in realtime.[168] Similarly, the National Security Agency is reportedly deploying sensors to monitor networks of critical infrastructure providers under a program called, in Orwellian fashion, "Perfect Citizen,"[169] although the NSA claims the system is only a vulnerability assessment tool.[170] Clarke and Knake propose that Internet users be required to use anti-virus programs on their computers,[171] and the vice president of Microsoft's Trustworthy Computing Group thinks consumers ought to have to produce an electronic "health certificate" before interacting with critical data online.[172] And, as previously described, proposals to alter the Internet's protocols to enable attribution have proliferated. The scope of code-based solutions, and who is responsible for determining that scope, remains a contested issue.

Existing proposals to address cybersecurity are rooted in dated theoretical approaches that are poorly suited to the issue's challenges. They range between highly radical, such as suggestions to give the U.S. President power to disconnect from the wider Internet, to painfully minimalist, such as bills that move cybersecurity responsibility among federal agencies like a shell game. These alleged reforms are reacting to a threat that is perceived to be immediate and grave. As the next Section describes, though, this perception is fundamentally flawed.

167. *See id.* at 241 ("Under the protection of PCII and through CIPAC, owners of critical infrastructure may share information with DHS about network intrusions without significant risk.").

168. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE INITIATIVE THREE EXERCISE 2–3 (2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf; Dawn Lim, *DHS Testing Einstein 3*, NEXTGOV (Apr. 8, 2010, 4:28 PM), http://techinsider.nextgov.com/2010/04/testing_of_einstein_3_underway_dhs.php.

169. Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J., July 8, 2010, at A3.

170. Lance Whitney, *NSA Offers Explanation of Perfect Citizen*, CNET (July 9, 2010, 12:53 PM), http://news.cnet.com/8301-1009_3-20010155-83.html.

171. CLARKE & KNAKE, *supra* note 23, at 165.

172. Robert McMillan, *Microsoft Has a Change of Heart on How to Keep Internet Safe*, ITWORLD (Feb. 15, 2011, 8:57 PM), http://www.itworld.com/security/137159/microsoft-has-a-change-heart-how-keep-internet-safe.

C. REALITY

The Internet is designed for exactly the challenge that cyberattacks produce: disruption to segments of the network that force re-routing of data, with the concomitant risk of lost information.[173] Moreover, there is good indirect evidence to believe that apocalyptic descriptions of cyberthreats are overdrawn. Accidents and natural disasters mimic the effects of deliberate disruption of Internet traffic. For example, undersea fiber-optic cables, which route much of the world's Internet data,[174] are routinely damaged or severed by events such as typhoons[175] and hurricanes.[176] Short-term effects can be significant: an earthquake in Taiwan in December 2006 cut four major fiber-optic cables, disrupting traffic moving east from Asia.[177] Taiwan's largest telecommunications company reported that ninety-eight percent of communication to Hong Kong, Malaysia, Singapore, and Thailand was taken offline.[178] When two undersea cables in the Mediterranean Sea were cut simultaneously in 2008, many Internet users in the Middle East and Asia were forced offline, including an estimated sixty percent of India's web services.[179] This example is particularly applicable, as affected network providers anticipated damage to only one cable at a time and employed the second cable as a precaution.[180] Damage to both cables more closely approximates the effects of

173. Electronic Frontier Foundation co-founder John Gilmore famously stated that "The Net interprets censorship as damage and routes around it." Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 64.

174. Heather Timmons, *Ruptures Call Safety of Internet Cables into Question*, N.Y. TIMES (Feb. 4, 2008), http://www.nytimes.com/2008/02/04/technology/04iht-cables.4.9732641.html.

175. *See, e.g.*, Dan Nystedt, *Typhoon Morakot Severs Three Undersea Cables*, PCWORLD (Aug. 12, 2009, 10:50 PM), http://www.pcworld.com/businesscenter/article/170126/typhoon_morakot_severs_three_undersea_internet_cables.html.

176. *See, e.g.*, Dan Nystedt, *Taiwan Earthquake Damages Undersea Internet Cables*, ITWORLD (Mar. 5, 2010, 7:40 AM), http://www.itworld.com/networking/99140/taiwan-earthquake-damages-undersea-internet-cables.

177. Ryan Singel, *Fiber Optic Cable Cuts Isolate Millions From Internet, Future Cuts Likely*, WIRED (Jan. 31, 2008, 8:59 AM), http://www.wired.com/threatlevel/2008/01/fiber-optic-cab/.

178. Chris Williams, *Taiwan Earthquake Shakes Internet*, THE REG. (Dec. 27, 2006, 10:13 GMT), http://www.theregister.co.uk/2006/12/27/boxing_day_earthquake_taiwan/.

179. Murad Ahmed, *India Suffers Massive Internet Disruption After Undersea Cables Break*, TIMES (Dec. 19, 2008), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5372294.ece.

180. *Id.*

a deliberate attack on the network. Similarly, the only fiber-optic cable running to West Africa was damaged in July 2009, causing significant impairment to Internet usage in Nigeria (which suffered loss of approximately seventy percent of its bandwidth), Togo, and Niger.[181] The March 2011 earthquake near Japan damaged undersea telecommunications cables and their associated routers, affecting Internet traffic in Asia.[182] The effects from these outages are similar to those of a cyberattack—indeed, there was speculation that the 2008 cable damage was caused by sabotage, with even the International Telecommunication Union advancing that theory.[183]

Hurricane Katrina had even greater effects on communications in the affected area of the southeastern United States in 2005; indeed, one researcher describes the storm as "the equivalent of a weapons of mass destruction (WMD) attack on the Gulf Coast."[184] The storm destroyed or disabled most communications capabilities in the area,[185] through a combination of physical damage (such as with cellular phone towers) and power outages (such as with landline phone service).[186] SCADA systems in utilities and other critical infrastructure were similarly disabled.[187] This multi-modal failure of critical infrastructure likely mimics the effects of a significant cyberattack.

However, even with major outages, data still flows. Within a few days of the 2006 Taiwan cable outage, alternative data paths were activated, international telephone links were restored, and Internet services came back on-line.[188] Physical re-

181. *Cable Fault Cuts off West Africa*, BBC NEWS (July 30, 2009, 10:48), http://news.bbc.co.uk/2/hi/8176014.stm.

182. Om Malik, *In Japan, Many Undersea Cables Are Damaged*, GIGAOM (Mar. 14, 2011, 10:34 AM), http://gigaom.com/broadband/in-japan-many-under-sea-cables-are-damaged/.

183. *Saboteurs May Have Cut Mideast Telecom Cables: UN Agency*, SYDNEY MORNING HERALD (Feb. 19, 2008, 3:50 AM), http://news.smh.com.au/technology/saboteurs-may-have-cut-mideast-telecom-cables-un-agency-20080219-1sv3.html.

184. Robert Miller, *Hurricane Katrina: Communications & Infrastructure Impacts*, *in* THREATS AT OUR THRESHOLD 191, 191 (Bert B. Tussing ed., 2006), *available at* http://www.gwumc.edu/hspi/policy/CHDSA2006.pdf.

185. *See, e.g.*, Heather K. Meeds, Communication Challenges During Incidents of National Significance: A Lesson from Hurricane Katrina 14 (Mar. 15, 2006) (unpublished student report, U.S. Army War College), *available at* http://www.strategicstudiesinstitute.army.mil/pdffiles/ksil424.pdf.

186. Miller, *supra* note184, at 193–94.

187. *Id.* at 194.

188. *See, e.g.*, Submarine Cable Protection—Experience of Hong Kong, China: Workshop and Information Sharing on Submarine Cable Protection,

pairs to the affected cables took longer, but were completed within fifty days.[189] Similarly, providers quickly re-routed traffic during disruptions caused by the 2008 cable incidents;[190] one Indian ISP restored service to normal levels within twenty-four hours.[191] The SAT-3 cable in West Africa that was damaged in 2009 was repaired within three weeks.[192] While poorer countries such as Niger, which rely solely on the SAT-3 cable, were effectively cut off from the Internet during this period, other states were able to shift to (admittedly more expensive) satellite links as an alternative.[193] Most networks in Louisiana, Mississippi, and Alabama were restored to service within several days of their initial outage, although a minority of networks remained persistently offline.[194] Japanese networks affected by the earthquake recovered quickly due to the country's "dense web of domestic and international connectivity."[195] Thus, while damage to Internet connectivity from disasters can be significant, it is also generally repaired rapidly.

There is a second source of data to evaluate the likely effects of a cyberattack: physical attacks. For example, the attack on Manhattan's World Trade Center towers on September 11, 2001, caused extensive damage to financial networks and data. The Verizon central switching office that serves most of lower Manhattan was damaged in the attack and in subsequent rescue efforts, cutting off 34,000 businesses and residences, and

OFFICE OF TELECOMMS. AUTH. (Apr. 13, 2009), http://www.ofta.gov.hk/en/speech-presentation/2009/20090413.pdf (PowerPoint presentation by Lawrence S M Kwan).

189. Singel, *supra* note 177.

190. *Third Undersea Internet Cable Cut in Mideast*, CNN (Feb. 1, 2008), http://www.cnn.com/2008/WORLD/meast/02/01/internet.outage/; Timmons, *supra* note 174.

191. Zafar Anjum, *India's VSNL Helps Restore Internet After Cable Break*, NETWORK WORLD (Feb. 6, 2008, 9:37 AM), http://www.networkworld.com/news/2008/020508-indias-vsnl-helps-restore-internet.html.

192. *Disrupted SAT3 Service Restored in West Africa*, BALANCING ACT (Aug. 21, 2009), http://www.balancingact-africa.com/news/en/issue-no-468/internet/disrupted-sat3-service-restored-in-west-africa.

193. *Cable Fault Cuts off West Africa*, *supra* note 181; *Internet Blackout in Niger: Niger's Dependence on the Damaged Beninese Fibre Optic Cable*, ASS'N FOR PROGRESSIVE COMMC'NS (Oct. 13, 2009), http://www.apc.org/en/news/internet-blackout-niger-niger-s-dependence-damaged.

194. James Cowie, et al., *Impact of Hurricane Katrina on Internet Infrastructure*, RENESYS, 4–5 (Sept. 9, 2005), http://www.renesys.com/tech/presentations/pdf/Renesys-Katrina-Report-9sep2005.pdf.

195. James Cowie, *Japan Quake*, RENESYS (Mar. 11, 2011, 7:20 PM), http://www.renesys.com/blog/2011/03/japan-quake.shtml.

severing 11,000 lines serving ISPs.[196] Even some companies that had invested in redundant Internet access lost transmission capabilities because their network providers routed the (putatively redundant) lines through the single Verizon physical plant.[197] Companies such as Hartford Financial Products suffered the complete physical destruction of their corporate headquarters and associated data center and information.[198]

Yet, even with this massive physical destruction of Internet capabilities, financial networks and companies returned to online operations rapidly. U.S. trading markets, such as the New York Stock Exchange, resumed normal operations six days after the attack.[199] Verizon began restoring some services as early as September 14.[200] Hartford Financial Products had its computers operating by September 14, and had moved into substitute offices by September 17.[201] The repair work necessary to restore communications was likely more extensive than would be required from a cyberattack, as it required not only resupply and routing of physical connectivity (in some cases up the sides of buildings), but also the reconstruction of Verizon's cable vault in the central office.[202]

Internet communication is thus quite hardy, particularly in America. Moreover, loss of routing is commonplace, and providers have experience managing the problem. Disruptions due to undersea cable damage, for example, are ubiquitous, though they affect primarily African nations with few alternative routing paths.[203] In the U.S., Internet-based service has proven to have greater resilience than other telecommunications meth-

196. GAO, GAO-03-414, POTENTIAL TERRORIST ATTACKS: ADDITIONAL ACTIONS NEEDED TO BETTER PREPARE CRITICAL FINANCIAL MARKET PARTICIPANTS 9, 37–39, 90–91 (2003), *available at* http://www.gao.gov/new.items/d03251.pdf.

197. *Id.* at 92–94.

198. *See* Julie Gallagher, *Importance of Redundancy, Diverse Systems Grows Post-9/11, Stresses Hartford Financial's Lowenthal*, INS. & TECH. (Oct. 24, 2001), http://www.insurancetech.com/architecture-infrastructure/14706497 (stating that the headquarters facility suffered "complete destruction," but also noting that the company maintained "a hot site in Boston" to protect critical information and records).

199. GAO, *supra* note 196, at 94.

200. *Id.* at 96.

201. Gallagher, *supra* note 198.

202. GAO, *supra* note 196, at 42–43.

203. John Borland, *Analyzing the Internet Collapse*, TECH. REV. (Feb. 5, 2008), http://www.technologyreview.com/Infotech/20152/; Ryan Singel, *Cable Cut Fever Grips the Web*, WIRED (Feb. 6, 2008, 1:50 PM), http://www.wired.com/threatlevel/2008/02/who-cut-the-cab/.

ods. For example, during Hurricane Katrina and subsequent flooding in Louisiana in 2005, landline telephone circuits, the State Police radio system, and cellular phone networks all failed.[204] One local ISP was able to maintain some Voice over Internet Protocol (VoIP) phone service even during the disaster, and the State Police used VoIP to communicate over their intranet (though traffic overwhelmed their network when they allowed unrestricted Internet use).[205] Indeed, one recommendation emerging from Katrina was that local law enforcement and government should move to an Internet (IP-based) architecture for emergency communication due to its robustness and flexibility.[206]

The Internet's core design anticipates that damage may occur to component networks. Thus, data routes dynamically, along the best available path at that moment.[207] TCP/IP does not guarantee packet delivery; indeed, packet loss is common, and is anticipated by applications that use the Internet.[208] In short, the Internet is designed for precisely the type of threat that cyberattacks pose. As one telecom analyst put it, "there will always be outages . . . . We are used to thinking of the Internet as being a thing that goes down."[209] While it is possible that a cyberattack could greatly reduce or eliminate Internet connectivity, it is unlikely. America in particular has robust, redundant connectivity to the rest of the world.

Even deliberate attempts by major ISPs to interfere with traffic flow as a competitive tactic fail. For example, in March 2008, Cogent Communications and the Swedish provider TeliaSonera stopped accepting traffic from each other's networks (known as "de-peering").[210] Cogent claimed that TeliaSonera failed to provide adequate bandwidth at interconnection points, and TeliaSonera argued that Cogent owed it compensation for

204. *National Science Board Workshop: Task Force on Hurricane Science and Engineering*, NAT'L SCI. FOUND., 5–6 (Apr. 18, 2006), http://www.nsf.gov/nsb/committees/archive/hurricane/3/henry.pdf (PowerPoint presentation by Robert R. Henry).

205. *Id.* at 5, 9.

206. *Id.* at 9.

207. JEFF DOYLE & JENNIFER CARROLL, ROUTING TCP/IP 131–41 (2006).

208. MATTHEW J. CASTELLI, NETWORK CONSULTANTS HANDBOOK 574 (2002).

209. Singel, *supra* note 177 (quoting Todd Underwood, a vice president of Renesys).

210. Ryan Singel, *ISP Quarrel Partitions Internet*, WIRED (Mar. 18, 2008, 4:00 PM), http://www.wired.com/threatlevel/2008/03/isp-quarrel-par/.

carrying traffic.[211] However, Swedes could still reach sites hosted on Cogent's network, and vice versa; it appears that the only entity made inaccessible by the dispute was Martha Stewart Living, and only from Sweden.[212] Other ISPs carried traffic between the warring firms, slowing access but enabling it to continue. Thus, even if a cyberattack were to disrupt a major ISP, or its connections to a peer, Internet access would likely continue largely unabated.

There is one key difference between natural disasters, and even some human-generated ones (such as the September 11 terror attacks): these disruptions are not adaptive, or ongoing. Though responders to Katrina, 9/11, and the Asian cable breaks faced challenging physical and communications conditions, they did not confront deliberate, changing impediments to their efforts.[213] A major cyberattack would likely attempt to degrade or prevent mitigation efforts, and could include physical attacks that would make rerouting efforts more difficult or impossible. Thus, existing disaster examples demonstrate one-off problems, but cannot show how Internet connectivity would respond to adaptive, ongoing attempts to disrupt it and to block repairs. Nonetheless, available data suggest that risks have been considerably overstated.

Even a significant cyberattack, though, would be more limited than commonly portrayed. Cybersecurity threats will be specifically targeted, rather than attacking the Internet as a whole. Claims to the contrary, while common, are either sloppy or simply wrong.[214] Moreover, there are at least two additional constraints that suggest attacks will target specific systems and information. First, some attackers—particularly nation-states—have significant Internet dependencies as well. China, for example, is linked into the global financial system via the Internet, and has integration in other economic sectors as

211. Tom Corellis, *Internet Rift Opens over ISP Peering Dispute*, DAILYTECH (Mar. 22, 2008, 8:15 AM), http://www.dailytech.com/Internet+Rift+Opens+over+ISP+Peering+Dispute/article11199.htm.

212. *Id.*

213. *See, e.g.*, Miller, *supra* note 184, at 200 (stating "with Katrina we had plenty of warning and we knew there wasn't likely to be a second onslaught . . . ."). *See generally* CLARKE & KNAKE, *supra* note 23, at 17–21 (describing Russian response to Georgian countermeasures during cyberattack).

214. Gable, for example, states that "[c]yberterrorists can attack the Internet itself." Gable, *supra* note 19, at 80.

well.[215] This point should not be overstated—political theorists famously predicted in the years before World War I that Europe's economies were too conjoined to permit conflict to erupt,[216] and attackers such as North Korea have little to lose if the Internet goes offline[217]—but the possibility of suffering self-inflicted damage should moderate the scope of attacks. This analysis accords with military theory suggesting that attackers generally leave room to escalate the level or severity of attacks, so as to push their enemy to quit the fight.[218] This "escalation dominance" would likely also influence a state launching cyberwar to focus its attacks, and to leave space for increased pressure.[219]

Second, a cyberattack on a country with military power, such as the United States, would invite reprisal in conventional (kinetic) terms even if attribution were only probabilistic or uncertain.[220] Indeed, after the alleged North Korean cyberattack on the U.S. and South Korea, the ranking Republican member of the Intelligence Committee of the House of Representatives called for a "show of force or strength" against that country, though North Korea's role was not free from doubt.[221] The broader the attack (and concomitant damage), the more likely that a response would involve conventional weapons.[222] In addition, an attack launched from computers in third-party countries, to disguise its origins, might cause those states to treat

215. *The Explosion of E-Commerce in China*, SEEKING ALPHA (Apr. 28, 2010), http://seekingalpha.com/article/201296-the-explosion-of-e-commerce-in-china.

216. *See, e.g.*, NORMAN ANGEL, THE GREAT ILLUSION—A STUDY OF THE RELATION OF MILITARY POWER TO NATIONAL ADVANTAGE (1912 ed.).

217. Martyn Williams, *North Korea Opens up Internet for National Anniversary*, COMPUTERWORLD (Oct. 9, 2010, 9:45 AM), http://www.computerworld.com/s/article/9190238/North_Korea_opens_up_Internet_for_national_anniversary (noting North Korea made its first full Internet connection in late 2010).

218. *See, e.g.*, FORREST E. MORGANET AL., DANGEROUS THRESHOLDS: MANAGING ESCALATION IN THE 21ST CENTURY 14–18 (2008).

219. *Cf.* HERMAN KAHN, ON ESCALATION: METAPHORS AND SCENARIOS 289–91 (Transaction Publishers 2010) (1965) (showing that the escalation dominance theory can apply to a broad set of circumstances).

220. The U.S. military claims to have improved its ability to determine responsibility for cyber attacks. Lolita C. Baldor, Associated Press, *Officials: U.S. Better at Finding Cyber Attackers*, THE GUARDIAN (Jan. 27, 2011), http://www.guardian.co.uk/world/feedarticle/9472832.

221. Kim Zetter, *Lawmaker Wants "Show of Force" Against North Korea for Website Attacks,* WIRED (July 10, 2009, 1:45 PM), http://www.wired.com/threatlevel/2009/07/show-of-force/.

222. *See* CLARKE & KNAKE, *supra* note 23, at 176–78.

the attacker as a belligerent, and possibly to carry out reprisals against it.

There is significant evidence to support these contentions. To date, hackers and spies have struck specific targets—for example, data on the U.S. Joint Strike Fighter,[223] funds in a bank's accounts,[224] overseas political opponents of a government,[225] or key equipment in a nuclear enrichment facility[226]—rather than assaulting Internet connectivity in general. In cases of cyberwar particularly, attackers have mounted assaults with a specific focus: combatants' systems, and their data. The cyberattack on Estonia sought to alter Web pages of that country's government, to prevent Estonian citizens from accessing news sites, and to discourage other countries from accepting Internet traffic from Estonia.[227] Even North Korea—commonly described as the state most likely to wage all-out cyberwar, given its limited information systems exposure to reprisal—has been judicious in its attacks so far.[228] The distributed denial of service attack attributed to North Korea aimed at specific targets: websites of selected U.S. government agencies, such as the Department of State and the Secret Service; major financial institutions such as the New York Stock Exchange; South Korean government websites; and South Korean banks. Clarke and Knake, whose book *Cyber War* argues that cyberattack threats are considerable in scale, call the North Korean attack "controlled" and "fairly sophisticated."[229] Cyberattackers are not nihilists. They have not sought to bring the Internet down as an end in itself. Rather, the Internet is a convenient pathway to accomplish their goals. Thus, cyberthreats are likely to target specific information or services on the Internet, rather than the network itself, and there are moderating factors that would restrain at least some attackers.

A more restrained and realistic view of cyberthreats is helpful to regulation. Available evidence on Internet damage

223. Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project,* WALL ST. J., Apr. 21, 2009, at A1.

224. Linda McGlasson, *NY Town's Bank Account Hacked*, BANK INFO SECURITY (Feb. 9, 2010), http://www.bankinfosecurity.com/articles.php?art_id=2182.

225. *Shadows in the Cloud*, *supra* note 62.

226. Broad et al., *supra* note 2.

227. Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&pagewanted=all.

228. *See* CLARKE & KNAKE, *supra* note 23, at 26–27.

229. *Id.* at 28.

strongly suggests that rushing to regulate is unnecessary, and potentially harmful. The Internet's fundamental design treats managing network disruptions, including from attacks, as a core goal. Cyberattacks would likely produce effects similar to other large-scale network problems, such as from natural disasters—they would slow traffic and increase costs, but routing would continue. In short, cyberspace is not falling, and overheated descriptions of cyberapocalypse obscure cybersecurity's true challenges. Policymakers have sufficient time to craft thoughtful solutions. Code is on their side. The next Section describes the approach that should guide their efforts.

III. TED STEVENS WAS RIGHT: CYBERSECURITY AS INFORMATION PROBLEM

Cybersecurity is, in truth, a problem of information. In this regard, Senator Ted Stevens was, ironically, correct: the Internet *is* a series of tubes.[230] Cybersecurity should concentrate on what flows through the tubes as its primary concern, rather than the tubes themselves. Indeed, such an orientation comports with the development principles of the Internet itself—the network is designed to be indifferent to the underlying connectivity that moves data from point to point. Users are unconcerned with how packets move across the Internet. They care only about their ability to send and receive them at the network's edge. This Article proposes that cybersecurity should concentrate on information, as evidenced by users' goals.

A. INFORMATION LAW'S HERITAGE

Focusing on information as the key tenet for regulation has a strong theoretical lineage, though it is relatively new to legal academia. Mary Graham has written on the use of information, and mandates for its provision, as a means of regulating problems from pollution to obesity.[231] Laws governing equity markets dictate the disclosure, and retention, of information about publicly traded corporations.[232] Trade secret statutes protect economically valuable private information to generate incen-

230. Senator Stevens' infamous quote is from a speech on network neutrality on June 28, 2006. *Series of Tubes*, YOUTUBE (June 28, 2006), http://www.youtube.com/watch?v=f99PcP0aFNE. The complete audio recording is available online, as well. Alex Curtis, *Senator Stevens Speaks on Net Neutrality*, PUBLIC KNOWLEDGE (June 28, 2006), http://www.publicknowledge.org/node/497.

231. *See generally* MARY GRAHAM, DEMOCRACY BY DISCLOSURE (2002).

232. *See, e.g.*, 17 C.F.R. §§ 210.2-06, 249.308 (2011).

tives for its production and use.[233] Scholarly debates about network neutrality concentrate not on the network's structure, but on how that structure affects the creation of information. Organizing research around information has revolutionized fields from behavioral biology,[234] to mathematics,[235] to economics.[236] An information-focused approach helped biologists explain why male peacocks developed ornate tails that make them easier targets for predators;[237] why rich single men publicly donate considerable sums to charity;[238] why spiders build decorations into their webs;[239] and why birds call loudly when doing so attracts the attention of raptors.[240] It explains why people spend so much free time on social networking sites.[241]

Similarly, economics is increasingly dominated by the study of information;[242] indeed, in 2001, the Nobel Prize for the field was awarded to three economists who pioneered the study

233. *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 260–83 (1998); David D. Friedman et al., *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 64 (1991).

234. *See, e.g.*, Thomas A. Sebeok, *A Communication Network Model for Languages is Applied to Signaling Behavior in Animals*, 147 SCI. 1006 (1965); Maynard J. Smith & D.G.C. Harper, *Animal Signals: Models and Terminology*, 177 J. THEORETICAL BIOLOGY. 305 (1995).

235. *See, e.g.*, C. E. Shannon, *A Mathematical Theory of Communication*, 27 BELL SYS. TECHNICAL J. 379 (1948) (extending the general theory of communication to include "the savings possible" by looking in part to the "statistical structure" of the information communicated).

236. *See, e.g.*, Michael Spence, *Job Market Signaling*, 87 Q.J. ECON. 355 (1973) (using market information to develop conceptual framework in economics).

237. *See, e.g.*, Amotz Zahavi, *Mate Selection—A Selection for a Handicap*, 53 J. THEORETICAL BIOLOGY 205, 210–11 (1975).

238. *See, e.g.*, Vladas Griskevicius et al., *Blatant Benevolence and Conspicuous Consumption: When Romantic Motives Elicit Strategic Costly Signals*, 93 J. PERSONALITY & SOC. PSYCHOL. 85, 85–86 (2007).

239. *See, e.g.*, Ren-Chung Cheng & I-Min Tso, *Signaling by Decorating Webs: Luring Prey or Deterring Predators?*, 18 BEHAV. ECOLOGY 1085, 1085 (2007).

240. *See, e.g.*, Carl T. Bergstrom & Michael Lachmann, *Alarm Calls as Costly Signals of Antipredator Vigilance: The Watchful Babbler Game*, 61 ANIMAL BEHAVIOUR 535, 535–36 (2001).

241. *See, e.g.*, Judith Donath, *Signals in Social Supernets*, 13 J. COMPUTER-MEDIATED COMM. 231, 231 (2008).

242. *See, e.g.*, Joseph E. Stiglitz, *Information and the Change in the Paradigm in Economics*, 92 AM. ECON. REV. 460, 460–61 (2002).

of asymmetric information in markets.[243] Behavior by market participants is increasingly explained by analyzing its informational content, from firms that offer product warranties,[244] to the difficulties of selling a used car,[245] to corporate decisions to offer shareholders a dividend.[246] Information economics explains why it is hard to sell an unsolicited script to a Hollywood movie studio,[247] or data on a bug to a software vendor.[248] Even wedding receptions play an informational role in social markets.[249] Economists have acknowledged information's power to shape markets—and vice versa—at least since F.A. Hayek's work on prices as aggregators of private data.[250] Increasingly, though, economic scholarship is oriented towards information as a principal focus.[251]

243. *The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2001*, NOBELPRIZE.ORG (2001), http://nobelprize.org/nobel_prizes/economics/laureates/2001/.

244. *See generally* William Boulding & Amna Kirmani, *A Consumer-Side Experimental Examination of Signaling Theory: Do Consumers Perceive Warranties as Signals of Quality?*, 20 J. CONSUMER RES. 111 (1993) (discussing signaling theory in the context of product warranty offerings).

245. *See generally* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970) (discussing how individuals use information in purchase decisions).

246. *See generally* Aharon R. Ofer & Daniel R. Siegel, *Corporate Financial Policy, Information, and Market Expectations: An Empirical Investigation of Dividends*, 42 J. FIN. 889 (1987) (discussing whether changes in corporate financial policy convey information about performance to the markets).

247. *See, e.g.*, Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CALIF. L. REV. 1293, 1366–68 (1996); Catherine L. Fisk, Screen Credit and the Writers Guild of America, 1938–2000: A Study in Labor Market and Idea Market Intermediation 3 (unpublished manuscript), *available at* http://www.law.nyu.edu/ecm_dlv1/groups/public/@nyu_law_website__engelberg_center_on_innovation_law_and_policy/documents/documents/ecm_pro_067662.pdf (discussing how credit for writing "establishes careers" and "affects how studios evaluate ideas").

248. Bambauer & Day, *supra* note 62, at 1063–65. *See generally* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609, 616 (Richard R. Nelson ed., 1962).

249. Francis Bloch el al., *Wedding Celebrations as Conspicuous Consumption: Signaling Social Status in Rural India*, 39 J. HUM. RESOURCES 675, 676 (2004).

250. *See generally* F. A. HAYEK, THE FATAL CONCEIT: THE ERRORS OF SOCIALISM 89–105 (W. W. Bartley III ed., paperback ed. 1991) (discussing how trade and commerce depend in part on individual or special information).

251. *See, e.g.*, Joseph E. Stiglitz, *The Contributions of the Economics of Information to Twentieth Century Economics*, 115 Q.J. ECON. 1441 (2000) (explaining how information economics has changed the way we think).

Mathematics, too, has shifted towards an information-centric approach, especially with game theory. This move began with the work of John von Neumann on games with both perfect[252] and imperfect[253] information, which he later applied to nuclear deterrence during the Cold War.[254] Mathematicians such as John Nash,[255] Norbert Wiener,[256] and Lloyd Shapley[257] refined and extended game theory. Game theory revolves around information: one's strategy is altered by what one knows about everyone else's strategies.[258] The mathematics of information have revolutionized approaches to problems as diverse as authenticating digital data,[259] voting manipulation,[260] dealing with rogue states,[261] and auctions of spectrum rights.[262] The key insight of game theory is that analysis must begin with assessing information, and in particular what information is accessible in a given system.[263]

252. J.v. Neumann, *Zur Theorie der Gesellschaftsspiele* [On Game Theory], 100 MATHEMATISCHE ANNALEN 295 (1928) (Ger.).

253. *See generally* JOHN VON NEUMANN & OSKAR MORGENSTERN, THEORY OF GAMES AND ECONOMIC BEHAVIOR (3d ed. 1953) (discussing the theory of games with both perfect and imperfect information).

254. *See, e.g.*, FLO CONWAY & JIM SIEGELMAN, DARK HERO OF THE INFORMATION AGE 252 (2005).

255. *See generally* John Nash, *Non-Cooperative Games*, 54 ANNALS OF MATHEMATICS 286 (1951) (applying game theory to poker).

256. *See generally* NORBERT WIENER, CYBERNETICS OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (1948) (explaining how information is used to provide effective control).

257. *See generally* L.S. Shapley, *A Value for n-Person Games*, *in* II CONTRIBUTIONS TO THE THEORY OF GAMES 307 (H.W. Kuhn & A.W. Tucker eds., 1953) (applying game theory to abstract games).

258. *See* JÜRGEN EICHBERGER, GAME THEORY FOR ECONOMISTS 16–17 (1993) (discussing the ways in which one's strategy is affected by his or her opponent).

259. *See generally* Gustavus J. Simmons, *A Game Theory Model of Digital Message Authentication*, 34 CONGRESSUS NUMERANTIUM 413 (1982) (using mathematical models to describe participant objectives in authentication games).

260. *See generally* ALAN D. TAYLOR, SOCIAL CHOICE AND THE MATHEMATICS OF MANIPULATION (2005) (presenting theorems of mathematical naturality that deal with the manipulability of voting systems).

261. *See generally* THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT (1960) (applying game theory to international conflicts).

262. PATRICK BAJARI & JEREMY T. FOX, MEASURING THE EFFICIENCY OF AN FCC SPECTRUM AUCTION 31 (2007), *available at* http://www.ftc.gov/be/seminardocs/bajarifox_auction.pdf.

263. *See* EICHBERGER, *supra* note 258 (discussing analysis of behavior in games of chess and penny matching and stating that "if optimal behavior of a player depends on the opponent's action, then the player needs to know what this opponent knows about the game and her behavior").

This Article draws upon information-based models in other scholarly fields to formulate a new theory of cybersecurity. The first critical, and difficult, step for this theory is to define what constitutes "information." At one level, every piece of data on the Internet, from Border Gateway Protocol messages to spam messages, constitutes information. However, this is not helpful: some of this data is already protected by wide distribution (for example, DNS information is frequently cached by servers),[264] and some of it does not require protection (for example, stateless protocols such as HTTP do not need to track requests, as they can be retransmitted).[265] This Article proposes a purposive definition of information: Internet data counts as information when it is something that users seek to access or engage with. A broker seeking the latest financial news from the *Wall Street Journal* is indifferent to the IP address of the Journal's website, and a bibliophile who wants to order Cormac McCarthy's *Blood Meridian* does not care whether Barnes and Noble is available at bn.com versus barnesandnoble.com. They care about accessing market news, or ordering the book. Information is the goal; data that route information to users are best understood as infrastructure. Information thus encompasses meta-data as well: it matters significantly to a user if an e-mail regarding her credit card bill resides in the "Paid" or "Unpaid" folder of her e-mail file. As we will see, information should be stored inefficiently; infrastructure need not be inefficient.

One can analogize the purposive definition of information to the distinction made in Fourth Amendment and privacy doctrine between routing data and content data: the words spoken during a phone call are content, while the number dialed is routing data.[266] The content/routing approach operates with a similar orientation to the new cybersecurity theory, as the distinction depends on whether the communicating party evinces a reasonable expectation of privacy in that signal.[267] Thus, it too focuses on user expectations. However, the distinction between routing data and content has, rightly, been criticized as collapsing at points.[268] There is both semantic and practical

264. DOUGLAS E. COMER, COMPUTER NETWORKS AND INTERNETS 74–75 (5th ed. 2009).

265. LEON SHKLAR & RICHARD ROSEN, WEB APPLICATION ARCHITECTURE 34 (2003).

266. *Compare* Katz v. United States, 389 U.S. 347 (1967) (content), *with* Smith v. Maryland, 442 U.S. 735 (1979) (routing data).

267. *Katz*, 389 UnitedStates at 361 (Harlan, J., concurring).

268. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO.

content value to learning a sender's e-mail address, even though that address is treated as routing data in constitutional[269] and statutory[270] privacy analyses. The e-mail address might well count as information, not infrastructure. Hence, the content/routing categories do not map perfectly; some material classified as routing data for privacy purposes could constitute information for cybersecurity purposes.

A simple test for the distinction between information and infrastructure is to consider how one would implement redundancy (as proposed in Part IV). Take, for example, the website for the White House. The site contains pages on President Obama's cabinet members, press briefings, policy issues, and presidential pets.[271] Its domain name is www.whitehouse.gov. Former cybersecurity czar Richard Clarke arranged for the White House site to be mirrored on Akamai's content caching servers to increase its redundancy, and hence security.[272] Thus, a user seeking a photo of President Obama's dog Bo on the White House site might in fact be connected to an Akamai server. The user is unconcerned about whether whitehouse.gov resolves to whitehouse.gov.edgesuite.net (an Akamai domain), but is (perhaps sadly) quite concerned about whether he can reach the picture of Bo at that address. Information is the material that a user expects to find, to view, or to make use of, regardless of where it is located. The domain name, IP address, server identity and physical location of the White House website may change, and are infrastructure. The photo of Bo is information.

This conceptually clean distinction may prove complicated in individual cases. One can argue whether a sender's e-mail address should be classified as information or as infrastructure,

WASH. L. REV. 1264, 1287–88 (2004). *But see* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1228 n.142 (2004).

269. *See, e.g.*, U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008).

270. 18 U.S.C. § 3121(c) (2006).

271. *See Issues*, THE WHITEHOUSE, http://www.whitehouse.gov/issues (last visited Nov. 7, 2011); *Presidential Pets*, THE WHITEHOUSE, http://www.whitehouse.gov/photos-and-video/photogallery/presidential-pets (last visited Nov. 7, 2011); *Press Briefings*, THE WHITEHOUSE, http://www.whitehouse.gov/briefing-room/press-briefings (last visited Nov. 7, 2011); *The Cabinet*, THE WHITEHOUSE, http://www.whitehouse.gov/administration/cabinet (last visited Nov. 7, 2011).

272. CLARKE & KNAKE, *supra* note 23, at 24, 112. A DNS query performed on February 19, 2011, indicates that www.whitehouse.gov is still hosted by Akamai, as the canonical name contains Akamai's edgesuite.net.

particularly given that such addresses are readily faked.[273] However, focusing on this question—whether given data counts as information—is precisely the point of this Article's approach. It evaluates cybersecurity by seeking to determine what content users want to engage with, rather than how it reaches them, or why. An information-oriented approach employing a purposive definition usefully re-orients cybersecurity towards users' needs.

Organizing cybersecurity around information has additional advantages. It provides a theoretical basis for developing responses, and for measuring their efficacy. Cybersecurity improves when authorized users can access the information they seek, and when unauthorized ones cannot. The information framework for cybersecurity is a functionalist one: it posits a set of goals or ends, and then measures possible responses based on how they achieve those ends.[274] At base, it is consequentialist, concerned more with outcomes than with the paths taken to reach them.[275] Moreover, the information-based approach comports with the underlying interests of Internet users, and sets aside more parochial concerns such as allocation of responsibility for enforcement, choice of regulatory methodology, or identification of malefactors.

Also, this theory avoids (or takes in passing) the welter of complications that ensues from standard scholarly approaches that try to sort behavior into the traditional categories of war, crime, terror and espionage based on an actor's identity and intent.[276] Consider, for example, a denial of service attack on a stock exchange's website.[277] The attack could be motivated by a desire to extort payments from the target (crime), by a nation-state seeking to interfere with key infrastructure (war), or by a violent non-state group making a political statement (ter-

273. *See* Bambauer, *supra* note 90, ¶¶ 14–15 (explaining how spam works based on trust between email domains).

274. On functionalism, see generally Michael J. Madison, *Notes on a Geography of Knowledge*, 77 FORDHAM L. REV. 2039, 2067–70 (2009) and Mark Tushnet, *The Possibilities of Comparative Constitutional Law*, 108 YALE L.J. 1225, 1238–69 (1999).

275. Information law can also be grounded in process-based deontological approaches. *See generally* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377 (2009).

276. *See, e.g.*, Brenner, *supra* note 17, at 404 (discussing complications in the threat dichotomy that arises from untraditional attacks in cyberspace).

277. *See, e.g.*, Devlin Barrett, *Hackers Penetrate NASDAQ Computers*, WALL ST. J., Feb. 5, 2011, at A1.

ror).[278] Hackers are skilled in concealing their tracks, and the Internet's architecture aids them in evading attribution. This deficit in identifying data stymies traditional scholarly models, which are left to call for better initial security (thereby wishing away the problem), and for alterations to the Internet that enhance attribution. Yet, while determining intent may help allocate responsibility for a response, it is ultimately irrelevant to the problem, which is that users cannot access information about their stocks on the exchange's site.[279] The information-based approach is both conceptually more precise, and more closely aligned to the purposes for which people access the Internet.

Next, this Article proposes three core concerns for its information-based theory of cybersecurity: access, alteration, and integrity.

B. ACCESS

Access to information measures whether users can obtain desired data via the Internet. Access can be conceived as a continuum with both a positive and negative range. In the positive direction, cybersecurity seeks to ensure that those who are authorized or intended to consume information are able to do so. In the negative direction, cybersecurity tries to prevent those who are not authorized to access data from doing so. Distributing information across multiple computers, for example, reduces the likelihood that an attacker can completely prevent access to that data.[280] Thus, the e-commerce firm Amazon thwarted the hacktivist group Anonymous by making use of the company's EC2 cloud computing service.[281] Anonymous was unable to overwhelm Amazon's legion of Web servers; consumers were still able to reach the site[282] and the hackers later publicly ad-

278. *See id.* (discussing that there are multiple motivations for hacking into the exchanges network).

279. *See, e.g.*, Gregg Keizer, *Russia's Stock Market Knocked Offline By DoS Attack*, INFO. W. (Feb. 3, 2006), http://www.informationweek.com/news/security/government/ 178601897.

280. *See, e.g.*, CLARKE & KNAKE, *supra* note 23, at 24, 112.

281. Paul McDougall, *Amazon Cloud Withstands WikiLeaks Attack*, INFO. W. (Dec. 9, 2010, 4:31 PM), http://www.informationweek.com/news/security/attacks/ 228800075.

282. Julianne Pepitone, *Why Attackers Can't Take Down Amazon.com*, CNNMONEY (Dec. 9, 2010, 2:35 PM), http://money.cnn.com/2010/12/09/technology/amazon_wikileaks_attack/index.htm.

mitted defeat.[283] Amazon's efforts demonstrate one effective means of addressing the positive aspect of access: overprovisioning ensured that those who wished to reach the site's information could do so.[284]

The negative aspect of access, though, is different: Amazon did not seek to prevent Anonymous from reaching its online store, but merely from blockading it. Cybersecurity also implicates access's negative range—on preventing undesired access to data. During the 2004 American presidential campaign, for example, the campaign website of President George W. Bush rejected access attempts from computers with non-U.S. IP addresses.[285] The Bush reelection campaign sought to limit access to the site's information to its target users: American voters. This concern is conceptually different from the positive aspect of access. It requires differentiating among requests for data, either by using proxies for permission (such as the user's IP address)[286] or directly by issuing credentials (such as name and password combinations, or cryptographic keys).[287] Blocking access can also be a blanket prohibition, such as when countries engage in statewide filtering of information.[288] China, for example, blocks all users on its network from accessing sites such as the official home page of the government of Taiwan, or that of the activist group Human Rights in China.[289] Thus, positive access requires ensuring that the right users can reach data, while negative access requires keeping the wrong users away from it.

283. *Id.*

284. Amazon's strategy is also effective in increasing the positive alteration aspect of cybersecurity, as discussed *infra* Part III.C.

285. *Geolocation filtering: www.georgewbush.com Blocked During Run-up to Election*, OPENNET INITIATIVE (Oct. 27, 2004), http://opennet.net/bulletins/007/.

286. *See, e.g.,* UEJF & LICRA v. Yahoo! Inc. & Yahoo! France, Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000 (Fr.), *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf (translation available at http://www.lapres.net/yahen.html) (noting that Yahoo! could block French users from accessing prohibited hate speech content based on IP address).

287. *See, e.g.*, David W. Chadwick & Alexander Otenko, *Implementing Role Based Access Controls Using X.509 Privilege Management—the PERMIS Authorisation Infrastructure*, *in* SECURITY AND PRIVACY IN ADVANCED NETWORKING TECHNOLOGIES 26, 38 (Borka Jerman-Blazic et al. eds., 2004) (showing how PERMIS provides an authorization engine which determines which users are allowed to perform which actions).

288. *See generally* Bambauer, *supra* note 275 (discussing internet censorship).

289. ACCESS CONTROLLED, *supra* note 95, at 21.

C. ALTERATION

Alteration similarly has positive and negative aspects. Alteration is separate from access, as one may access information without being able to alter it, and vice-versa. A user can read stock price updates from the New York Stock Exchange without having the capability to alter that information. Similarly, a citizen who engages in electronic voting has the power to alter the underlying information (the total votes cast, as well as the number cast for a particular candidate) without having the capacity to access it.[290] I can send you an e-mail message, thereby changing your Inbox, without being able to access your Inbox. The positive range of alteration seeks to ensure that authorized users can change information. Facebook, for example, was unavailable to people attempting to post status updates, or to indicate how much they "like" a Web page, for nearly three hours in September 2010—an example of trivial importance, but one of wide incidence, as the social network boasts over 500 million users.[291] Less trivially, the ability to alter information is at the root of electronic commerce, messaging, and financial data exchange. Positive alteration concerns include ensuring that the data to be updated is available, and that authorized users can make changes to it.

Cybersecurity's negative range for alteration focuses on preventing changes to information by unauthorized users. This could involve preventing the wholesale deletion of data, such as occurred when U.K. Internet Service Provider VAServ lost the contents of over 100,000 hosted sites due to hacking in June 2009.[292] The hackers gained root access on the system, allowing them to delete files; the loss was particularly problematic for customers subscribing to VAServ's lower-cost unmanaged service, where data was not backed up systematically.[293] One might also view Amazon's deletion of the George Orwell novel *1984* from its customers' Kindle e-book readers as unauthorized alteration (although Amazon claimed refuge in boilerplate au-

290. *See generally* Ronald L. Rivest, *Electronic Voting*, MASS. INST. TECH. http://people.csail.mit.edu/rivest/Rivest-ElectronicVoting.pdf (last visited Nov. 7, 2011).

291. Jennifer Valentino-DeVries, *What Caused Facebook's Worst Outage in Four Years*, WALL ST. J. BLOG (Sept. 24, 2010, 10:50 AM), http://blogs.wsj.com/digits/2010/09/24/what-caused-facebooks-worst-outage-in-four-years.

292. Dan Goodin, *Webhost Hack Wipes Out Data for 100,000 Sites*, THE REG. (June 8, 2009, 8:02 PM), http://www.theregister.co.uk/2009/06/08/webhost_attack/.

293. *Id.*

thorization language in the Kindle terms of service agreement).[294] Unauthorized alteration could also come in the form of changes to information, rather than its complete erasure. For example, the hacker group Iranian Cyber Army left virtual graffiti on the home page of China's Baidu search engine in January 2010, replacing its usual appearance with an image of Iran's flag.[295] The Stuxnet cyberweapon replaced actual centrifuge data with faked information indicating the machines were operating normally, lulling Iran's nuclear engineers into a false sense of security.[296] While it is easy to recognize when a website has been defaced, unauthorized alteration of information could be more subtle, and difficult to detect, as Stuxnet demonstrates.

Lastly, the information-based theory raises a second-order concern: data integrity. This issue arises after a user seeks either to access or alter information. The concern is whether the user is interacting with valid, up-to-date information. In distributed computing systems, such as where websites are cached to improve access speeds, either users must accept that data will be stale (though perhaps only slightly so), or systems must devise ways to rapidly propagate changes to each copy of the information.[297] Thus, when most users load CNN.com in their Web browser, the page returned comes not directly from CNN's servers, but instead from a copy cached by Akamai.[298] Users, and CNN itself, trade accuracy for speed. For some purposes, though, such as financial transactions, using real-time data is critical. Financial companies build expensive high-speed networks to ensure that information is up-to-date.[299] The London

294. Brad Stone, *Amazon Erases Orwell Books From Kindle*, N.Y. TIMES, July 18, 2009, at B1; Mark Hachman, *Amazon's Bezos Apologizes for '1984' Kindle Boondoggle*, PCMAG.COM (July 24, 2009, 7:18 PM), http://appscout.pcmag.com/mobile-apps/272034-amazon-s-bezos-apologizes-for-1984-kindleboondoggle#fbid=UEnYsvQkesW.

295. Melanie Lee, *China's Baidu Website Defaced by Twitter Hackers*, REUTERS, Jan. 12, 2010, *available at* http://www.reuters.com/article/2010/01/12/china-hacking-idUSTOE60B05U20100112.

296. See supra notes 2–6 and accompanying text.

297. *See, e.g.*, Geoff Huston, *Web Caching*, 2 INTERNET PROTOCOL J. 2 (1999), *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_2-3/ipj_2-7.pdf.

298. *See, e.g.*, Press Release, CNN.com Teams with Akamai to Deliver Record Traffic on Election Day, (Nov. 10, 2004), *available at* http://www.akamai.com/html/about/press/releases/2004/press_111004.html.

299. Charles Duhigg, *Stock Traders Find Speed Pays, in Milliseconds*, N.Y. TIMES, July 24, 2009, at A1.

Stock Exchange replaced its matching engine because the software experienced delays of up to 2 milliseconds; the new Linux-based engine operates with an average latency of only 125 microseconds.[300] High-frequency trading executes orders in a few hundred microseconds—these trades occur so rapidly that the physical location of the server executing them affects their timing.[301] Similarly, cybersecurity must consider how to signal to users whether a given piece of information reflects the most recent set of authorized changes.

Integrity also requires providing a method to determine whether information, including up-to-date information, is valid—whether it encompasses only authorized changes. The Stuxnet worm exemplifies this concern: it caused Iran's centrifuges to relay inaccurate information, concealing the weapon's effects on the uranium enrichment process.[302] Author Tom L. Clancy offered another example, before the Internet was in widespread use, in his 1995 novel *Debt of Honor*. In the book, operatives covertly falsify data on the New York Stock Exchange trading system during a conflict between Japan and the U.S., leading to a financial panic. Traders are unable to determine what information is valid, leading to economic chaos.[303] To prevent similar real-world problems, the information-based approach posits that cybersecurity must incorporate mechanisms to determine whether a given datum's state reflects only authorized changes.

D. INTEGRITY

Finally, information integrity must grapple with changes in distributed data stores. When information resides in multiple locations, it is possible—perhaps even likely—that authorized users will make changes to different copies at the same

300. Leo King, *London Stock Exchange Price Data Failures 'Emerged Immediately at Millennium Launch'*, COMPUTERWORLD UK (Feb. 18, 2011, 5:40 PM), http://www.computerworlduk.com/news/it-business/3261816/london-stock-exchange-price-data-failures-emerged-immediately-at-millennium-launch.

301. Jacob Aron, *High-Speed Trading Algorithms Place Markets at Risk*, NEW SCIENTIST (July 8, 2011, 3:39 PM), http://www.newscientist.com/blogs/onepercent/2011/07/high-speed-trading-algorithms.html?DCMP=OTC-rss&nsref=online-news.

302. See supra notes 2–6 and accompanying text.

303. Clarke and Knake contemplate a similar scenario and recommend Clancy's solution: rolling back data to the last known valid state. CLARKE & KNAKE, *supra* note 23, at 204.

time.[304] Distributed database systems such as Lotus Notes must incorporate mechanisms for resolving these disparities during updates.[305] At minimum, systems must be capable of choosing which copy counts as the most up-to-date valid instantiation of the data. Optimally, an information-based approach would provide means for reconciling conflicting changes, and of tracking the history of alterations to each copy.[306]

Fortunately, the computer science literature offers numerous techniques to accomplish these functions. For example, cryptographic hash functions enable the use of manipulation detection codes, whereby one can detect alteration to a given data set.[307] Voting-based methods compare multiple instances of a data set; the version with the greatest number of instantiations is treated as correct.[308] To understand voting, imagine three instances of a CNN.com headline. Two read "Truman Defeats Dewey"; one reads "Dewey Defeats Truman." The first version, where Truman wins, has more "votes" and thus counts as the correct version. Similarly, message digest functions can validate integrity even in challenging technical environments such as peer-to-peer media streaming.[309] In addition, programs such as BitTorrent,[310] Lotus Notes,[311] mySQL,[312] and Oracle

304. Formally, these would be different updates even if the underlying data change made by each user were the same (such as altering a bit from a value of 1 to 0), as each change has a different provenance.

305. *See Replication and Save Conflicts*, IBM, http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp?topic=/com.ibm.help.domino.admin.doc/DOC/H_ABOUT_REPLICATION_AND_SAVE_CONFLICTS.html (last updated Oct. 5, 2009) (providing directions on reducing replication or save conflicts).

306. *Id.*; *see also* Todd L. Graves et al., *Predicting Fault Incidence Using Software Change History*, 26 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 653 (2000) (using statistical models to evaluate which characteristics lead to a large number of faults).

307. *See* ALFRED J. MENEZES ET AL., HANDBOOK OF APPLIED CRYPTOGRAPHY 321–67 (1997).

308. *See, e.g.*, Johannes Osrael et al., *Adaptive Voting for Balancing Data Integrity with Availability*, *in* ON THE MOVE TO MEANINGFUL INTERNET SYSTEMS 2006: OTM 2006 WORKSHOPS 1510, 1510–18 (Robert Meersman et al. eds., 2006) (discussing replication of data for maintaining system availability and various voting methods employed to determine the correct data set).

309. Ahsan Habib et al., *Verifying Data Integrity in Peer-to-Peer Media Streaming*, *in* MULTIMEDIA COMPUTING AND NETWORKING 11 (Surendar Chandra et al. eds., 2005).

310. BitTorrent uses a cryptographic hash to allow nodes to detect whether a piece of a requested file has been modified. *See* Andrew Loewenstern, *DHT Protocol*, BITTORRENT.ORG, http://www.bittorrent.org/beps/bep_0005.html (last updated Feb. 28, 2008).

Fusion[313] implement such techniques. Thus, there is a body of both theoretical methods and software implementation examples for cybersecurity to draw upon in dealing with information integrity.

E. REORGANIZING CYBERSECURITY

This new theory, with its focus on accessing, altering, and verifying the integrity of information, usefully illuminates the flaws in current scholarly approaches that concentrate on identity and intent. As the following table makes clear, traditional methodologies classify the same actions, and effects on information, differently depending on who carries them out, and for what purpose. This may be helpful for second-order reasons, such as whether a response to an attack falls within the purview of military or civilian authorities. However, it reifies these concerns at the expense of core issues of cybersecurity. When users are prevented from reaching critical information, they are less concerned with the identity and goals of those responsible than with having access restored. Similarly, if someone makes unauthorized changes to information, those who want to use it will be more focused on restoring that data to its last known valid state than on parsing why it was altered. Information wants to be used. The information-based approach to cybersecurity concentrates on those uses.

Information-Based Theory	**Identity/Intent-Based Theories**
Positive Access (ensure authorized access)	Crime (ransomware) Terrorism (denial of service) War (denial of service)
Negative Access (prevent unauthorized access)	Espionage (data theft/intelligence gathering) Crime (IP theft)
Positive Alteration (ensure authorized changes)	Crime (distributed denial of service) Terrorism (denial of service) War (denial of service)

311. *Replication and Save Conflicts*, *supra* note 305 (providing directions on consolidating replication or save conflicts).

312. Robin Schumacher, *Guaranteeing Data Integrity with MySQL 5.0*, MYSQL, http://kambing.ui.ac.id/mysql/tech-resources/articles/mysql-data-integrity.html (last visited Nov. 7, 2011).

313. *Solving Common Replication Conflicts*, ORACLE, http://download.oracle.com/docs/cd/E20295_01/html/821-1220/bcasp.html (last visited Nov. 7, 2011).

Negative Alteration (prevent unauthorized changes)	Crime (hacking/data deletion) Terrorism (hacking/data deletion) War (hacking/data deletion)

The information-based approach to cybersecurity also strongly suggests that there are tradeoffs among security goals. Specifically, regulators are likely to be forced to choose between emphasizing the positive aspects of alteration and access, and the negative aspects. Creating more ways for users to reach and interact with information will, of necessity, generate more pathways for malfeasors to reach that information as well. This Article focuses upon a conceptual approach to improving the positive aspects of cybersecurity through inefficiency. Future work will address cybersecurity's negative aspects. The next Part describes why, ironically, *in*efficient data storage and connectivity is useful for positive access and alteration, and then turns to the inevitable tradeoffs that this approach entails.

IV. INEFFICIENCY'S VIRTUES

For cybersecurity's positive aspects, inefficiency reigns. This is counterintuitive. Efficiency is nearly the Holy Grail of computer science, from increasing the speed of search algorithms[314] to improving the storage of data on disk.[315] Companies spend considerable sums to gain tiny improvements in efficiency.[316] Financial firms invested hundreds of millions of dollars[317] in computers, low-latency network connections, and proprietary algorithms[318] to increase the speed of trades by a few milliseconds. The payoff is estimated to be $21 billion an-

314. *See generally* STEPHEN WISE, GIS BASICS 76–84 (2002) (describing algorithm efficiency).

315. *See, e.g.*, P. Chicoine et al., *Hard Disk Drive Long Data Sector White Paper*, IDEMA, 8–9 (Apr. 20, 2007), http://www.idema.gr.jp/technical/white/6_13_07.pdf (describing efficiency gains from conversion to Advanced Format disk storage format).

316. Duhigg, *supra* note 299 (describing how stock traders invest money to gain improvements in efficiency).

317. Rick Bookstaber, *The Arms Race in High Frequency Trading*, RICK BOOKSTABER (Apr. 21, 2009), http://rick.bookstaber.com/2009/04/arms-race-in-high-frequency-trading.html.

318. *See, e.g.*, Jack Lynch, *Programmer Indicted in Goldman Code Theft Case*, N.Y. TIMES DEALBOOK BLOG (Feb 11, 2010, 4:49 PM), http://dealbook.blogs.nytimes.com/2010/02/11/programmer-indicted-in-goldman-code-theft-case (discussing theft of proprietary software and its seriousness).

nually.[319] Efficiency determines adoption of technological standards. Apple refuses to support the near-ubiquitous Flash video format on its mobile products,[320] due primarily to efficiency concerns. Former chief executive Steve Jobs called Flash a "CPU hog,"[321] and his official statement noted the company's conclusion that "[f]lash has not performed well on mobile devices."[322] Similarly, concerns over compression efficiency of competing video codecs blocked adoption of one codec as a standard in HTML5.[323] In short, seeking to increase efficiency in computing is the norm, and a proposal to deliberately cultivate inefficiency is admittedly unusual.

Moreover, this pro-efficiency bias is particularly true for the Internet. The Internet's core design frequently sacrifices countervailing considerations in favor of efficiency. For example, Internet Protocol does not perform error-checking when routing data packets.[324] Any packets that go missing must be re-transmitted. This "best efforts" model forgoes delivery guarantees to optimize IP for efficient data transfer.[325] Internet protocols sometimes must select for efficiency in certain tasks at the expense of others. For example, the Domain Name System (DNS) uses a distributed database to map domain names to IP addresses.[326] This mapping improves the efficiency of responding to requests since there are more DNS servers to share the load, some of which will be "closer" on the network to the requester.[327] However, the distributed database detracts from the efficiency of propagating changes. When IBM changes the IP address for the Web server that hosts www.ibm.com, that

319. Rob Iati, *The Real Story of Trading Software Espionage*, ADVANCED TRADING (July 10, 2009), http://advancedtrading.com/algorithms/ 218401501.

320. Stephen Shankland, *Jobs: Why Apple Banned Flash from the iPhone,* CNET NEWS (Apr. 29, 2010, 6:56 AM), http://news.cnet.com/8301-30685_3-20003739-264.html.

321. Erica Ogg, *Report: Jobs Disses Adobe Flash as "CPU Hog"*, CNET NEWS (Feb 18, 2010, 2:31 PM), http://news.cnet.com/8301-31021_3-10456175-260.html.

322. Steve Jobs, *Thoughts on Flash*, APPLE (Apr. 2010), http://www.apple.com/hotnews/thoughts-on-flash.

323. Ryan Paul, *Decoding the HTML5 Video Codec Debate*, ARS TECHNICA (July 5, 2009), http://arstechnica.com/open-source/news/2009/07/decoding-the-html-5-video-codec-debate.ars.

324. INFO. SCIS. INSTIT., RFC 791: INTERNET PROTOCOL 2 (Jon Postel ed., Sept. 1981), *available at* http://www.rfc-editor.org/rfc/rfc791.txt.

325. *See, e.g.*, CHARLES M. KOZIEROK, THE TCP/IP GUIDE 690 (2005).

326. CRICKET LIU & PAUL ALBITZ, DNS AND BIND 3–10 (2006).

327. *See* KOZIEROK, *supra* note 325, at 849 (explaining that this distribution of data leads to efficiency and reliability).

change must be updated in the caches of many DNS servers, whereas employing a single, centralized database would ensure an instantaneous update.[328] While trade-offs between goals are inevitable, the underlying principle of maximizing efficiency is widely implemented.

Yet cybersecurity is different. Maximizing users' ability to access and alter information is best achieved through inefficient storage and inefficient network connections. Having information located in multiple places makes it more costly to maintain. However, it is also more resilient. A single information repository efficiently scales to serve many users, and updates must only be made once. But if attackers discover a vulnerability, such as a zero-day attack that affects the monolith, all may be lost.[329]

Similarly, having a single high-speed network can be highly efficient, until a glitch or attack knocks it offline. Beth Israel Deaconess Medical Center in Boston had a state-of-the-art network built by Cisco Networks to connect its doctors to medical data such as electronic health records.[330] Yet, when a researcher's program flooded the network, the hospital's data access was cut off.[331] For the next four days, staff wrote orders on paper and delivered them by hand while technicians worked feverishly.[332] Having a single point of failure in its computing infrastructure forced the hospital to shift information normally carried by 100,000 daily e-mails onto paper.[333] In the aftermath, Beth Israel Deaconess spent $3 million on upgrading its technology—specifically, building a second, parallel network.[334]

328. *Cf.* NAT'L RES. COUNCIL, SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEM AND INTERNET NAVIGATION 43 (2005) (showing how "the work of registering changes [in a DNS model] is distributed among many organization," and therefore, could inherently not be instantaneous (although it may be less burdensome to each individual organization)).

329. *See, e.g.*, Goodin, *supra* note 292 and accompanying text (discussing the destruction of 100,000 websites as a result of a zero-day vulnerability in a widely used virtualization application).

330. Anne Barnard, *Got Paper? Beth Israel Deaconess Copes with a Massive Computer Crash*, BOS. GLOBE, Nov. 26, 2002, at C1; *see also* Peter Kilbridge, *Computer Crash–Lessons from a System Failure*, 348 NEW ENG. J. MED. 881, 881 (2003) (explaining the variety of network applications available to doctors and patients).

331. Barnard, *supra* note 330 (describing the crisis faced by the medical center when its system froze).

332. Michele Kurtz, *His Goal: Computerized Patient Records*, BOS. GLOBE, Aug. 24, 2004, at C2.

333. Barnard, *supra* note 330.

334. *Id.*

The network failure was caused initially by bad code—described in news reports as a "virus," though a self-inflicted one—but in a larger sense was caused by the hospital's decision to opt for efficiency over redundancy.[335]

Inefficiency creates resiliency. Data stored in many places gives users more locations to access and alter it. Providing many paths to reach that information improves users' chances of doing so. It can also serve to deter attacks by muting their effects. There is little benefit to launching a fruitless attack. Thus, inefficiency improves the positive aspects of cybersecurity. The next two sections of this Article describe how to implement inefficiency for information and for connectivity.

A. SCATTERING THE BITS

WikiLeaks survives.

Like the hydra, each time an attack cuts off one of WikiLeaks's heads, another sprouts. In 2008, a federal judge ordered WikiLeaks's domain name registrar to sever the site's link to its wikileaks.org domain name.[336] Users who entered wikileaks.org into their browser would not reach Julian Assange's repository. Undaunted, the site shifted to a new domain name to evade the block, and the judge eventually surrendered and dissolved the injunction.[337] In late 2010, after posting a massive batch of U.S. diplomatic cables and military documents, WikiLeaks was dropped as a customer of Amazon's cloud computing service, forcing the site to find a new Web host.[338] Its DNS provider, under pressure from a denial of ser-

335. *See* Kurtz, *supra* note 332 (using "virus" description to explain the computer's network problem); *see also* E-mail from Richard M. Smith to Declan McCullagh (Dec. 3, 2002, 06:49), *available at* http://seclists.org/politech/2002/Dec/4 (noting that "the wounds however were self-inflicted").

336. Order Granting Permanent Injunction, Bank Julius Baer & Co. v. WikiLeaks, No. CV08-0824 (N.D. Cal. Feb. 15, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv00824/200125/48/. The order banned Dynadot from translating requests for the wikileaks.org domain name to the relevant IP address. *Id.*

337. Order Denying Motion for Preliminary Injunction; Dissolving Permanent Injunction; And Setting Briefing and Hearing Schedule, *WikiLeaks*, 535 F. Supp. 2d 980, 985–86 (N.D. Cal. 2008).

338. *See* Geoffrey A. Fowler, *Amazon Says WikiLeaks Violated Terms of Service*, WALL ST. J. (Dec. 3, 2010), http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html (explaining that WikiLeaks was dropped for breaking Amazon's rules of service).

vice attack, terminated WikiLeaks as a client.[339] The payment providers MasterCard and PayPal ceased processing payments to WikiLeaks.[340] A patriotic hacker launched a cyber attack against WikiLeaks that knocked WikiLeaks offline for a time.[341] Yet, through all of these tribulations, WikiLeaks' trove of information remained available, mirrored on thousands of sites at a host of domain names.[342] Users seeking information about Australia's black list of filtered websites[343] or the Church of Scientology's financial status[344] can access such material with ease. WikiLeaks accomplishes this remarkable persistence through inefficiency: the site's information is widely duplicated, ensuring that no single attack can prevent access or alteration (such as submitting new documents). WikiLeaks's information lives on multiple servers, including a server located in a former nuclear bunker in Stockholm, Sweden,[345] on the Swedish Pirate Party's servers,[346] and on the computers of

339. Charles Arthur & Josh Halliday, *WikiLeaks Fights to Stay Online After US Company Withdraws Domain Name*, THE GUARDIAN, (Dec. 3, 2010), http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns.

340. *See* Declan McCullagh, *MasterCard Pulls Plug on WikiLeaks Payments*, CNET NEWS (Dec. 6, 2010, 2:37 PM), http://news.cnet.com/8301-31921_3-20024776-281.html (describing MasterCard's decision to stop accepting WikiLeaks payments); Alexia Tsotsis, *PayPal VP on Blocking WikiLeaks: State Department Said It Was Illegal*, TECHCRUNCH (Dec. 8, 2010), http://techcrunch.com/2010/12/08/paypal-wikileaks/ (discussing PayPal's decision to block WikiLeaks payments).

341. Richard Allen Greene & Nicola Hughes, *'Hacktivist for Good' Claims WikiLeaks Takedown*, CNN (Nov. 29, 2010), http://www.cnn.com/2010/US/11/29/wikileaks.hacker/index.html?hpt=T1.

342. *See* Brian Prince, *WikiLeaks Hit with DoS Attack Before Documents Leaked*, EWEEK.COM (Nov. 29, 2010), http://www.eweek.com/c/a/Security/WikiLeaks-Hit-With-DoS-Attack-Before-Documents-Leaked-680058/ (crediting WikiLeaks's ability to avoid significant downtime to its decision to use three IP addresses since its launch).

343. *See Australian Government Secret ACMA Internet Censorship Blacklist, 18 Mar 2009*, WIKILEAKS (Mar. 20, 2009), http://www.wikileaks.info/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist,_18_Mar_2009 (providing a list of the Australian Communication and Media Authority's "internet censorship blacklist").

344. *Scientology Cult Finance Documents Part 1*, WIKILEAKS (Apr. 9, 2008), http://www.wikileaks.org/wiki/Scientology_cult_finance_documents_part_1.

345. Andy Greenberg, *WikiLeaks Servers Move to Underground Nuclear Bunker*, FORBES (Aug. 30, 2010), http://blogs.forbes.com/andygreenberg/2010/08/30/wikileaks-servers-move-to-underground-nuclear-bunker/?boxes=businesschanneltopstories.

346. *Swedish Pirate Party to Host WikiLeaks Servers*, CNN (Aug. 18, 2010), http://edition.cnn.com/2010/WORLD/europe/08/18/sweden.wikileaks/.

OVH, a French web services company.[347] Changes to WikiLeaks must propagate across these doppelgangers, but the inefficient nature of the site's storage increases its security. WikiLeaks arrived at this information architecture through hard experience: the site has experienced cyberattacks,[348] law enforcement pressure,[349] and even threats of assassination against Assange.[350] WikiLeaks is a test case for increasing cybersecurity through information inefficiency. And the results are clear: inefficiency works.

This Article's information-oriented theory posits that a key goal for cybersecurity is increasing the inefficiency with which information is stored. The positive aspects of both access to, and alteration of data, emphasize the need to ensure that authorized users can reach, and modify, information. This is more likely to occur when users can reach data at multiple locations, both because it increases attackers' difficulty in blocking their attempts, and because it provides fallback options if a given copy is not available. In short, data should reside in many places.

This approach to implementing the information-oriented theory of cybersecurity aligns with prior proposals and efforts. Jonathan Zittrain suggests that there should not be single, monolithic Internet repositories of information.[351] Instead, he proposes, Web hosts and other ISPs should adopt a communitarian ethic of caching data as they relay it in response to user requests.[352] Richard Clarke replicated the White House's web-

347. Associated Press, *French Company Allowed to Keep Hosting WikiLeaks*, YAHOO! FIN. (Dec. 8, 2010, 7:37 AM), http://finance.yahoo.com/news/French-company-allowed-to-apf-1530963796.html?x=0.

348. *See* Greene & Hughes, *supra* note 341 (discussing a hacker who took WikiLeaks's site down for political reasons).

349. *See, e.g.*, *Assange Attorney: Secret Grand Jury Meeting in Virginia on WikiLeaks*, CNN (Dec. 13, 2010), http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?_s=PM:CRIME (discussing a criminal investigation into WikiLeaks's publication of diplomatic cables).

350. *See* Jeffrey T. Kuhner, *Assassinate Assange?*, WASH. TIMES, Dec. 3, 2010, http://www.washingtontimes.com/news/2010/dec/2/assassinate-assange/ (stating that "Mr. Assange is not a journalist or publisher; rather, he is an enemy combatant - and should be treated as such" and that "[t]he administration must take care of the problem").

351. *See* Zittrain, *supra* note 105, at 2777–78 (arguing that eliminating monopolistic repositories of information "creates a useful friction in the system, while still preserving opportunity for removing material").

352. *See id.* at 2779–81 (explaining the benefits of such a system by saying that "[i]f one site later fails or is blocked, the user can request a copy of it from the server that linked him there").

site on Akamai's servers, allowing the site to remain available even during a denial of service attack in July 2009.[353] The BitTorrent peer-to-peer application spreads data across its network of nodes so that any one computer holds only a small fragment of a particular file.[354] Each BitTorrent host thus incurs a minimal burden when sharing files, and requests for a given file do not depend on any single node's availability.[355] For e-mail, organizations often employ multiple servers corresponding to a single domain name to ensure that messages reach their destination even if one computer fails.[356]

Most entities that store information deliberately make their storage redundant; indeed, such efforts may be legally mandated. Attorneys licensed to practice in New York, for example, must maintain certain bookkeeping records for seven years after a client matter ends.[357] U.S. Securities and Exchange Commission regulations dictate that accounting firms keep records related to auditing and financial statement review for seven years after such reviews are concluded.[358] The Health Insurance Portability and Accountability Act requires that certain health information be retained for at least six years.[359] The Food and Drug Administration imposes requirements, under its Good Manufacturing Standards, that certain medical device data be preserved for at least two years from the date the data is released for commercial distribution.[360] The Occupational Health and Safety Act institutes a requirement that data on employees' workplace exposure to hazardous or toxic substances be maintained for at least thirty years.[361] These existing requirements suggest that private incentives for information storage are frequently inadequate, at least in comparison to larger societal interests in that information. Moreover, cybersecurity regulation of information inefficiency can effectively

353. *See* CLARKE & KNAKE, *supra* note 23, at 24.

354. *See, e.g.*, MATTHEW RIMMER, DIGITAL COPYRIGHT AND THE CONSUMER REVOLUTION: HANDS OFF MY IPOD 113–15 (2007) (explaining BitTorret and describing it as a "file distribution tool").

355. For an argument that BitTorrent's file-sharing architecture is faster and more efficient than traditional networking sites, see *id.* at 113.

356. This technique involves listing multiple mail exchange, or MX, records for a given host name in the Domain Name System. *See* LIU & ALBITZ, *supra* note 326, at 89–99 (explaining the effect of DNS on electronic mail).

357. N.Y. RULES OF PROF'L CONDUCT R. 1.15(d) (2009).

358. 17 C.F.R. § 210.2-06 (2011).

359. 45 C.F.R. § 164.530(j)(2) (2010).

360. 21 C.F.R. § 820.180(b) (2011).

361. 29 C.F.R. § 1910.1020(d)(1)(ii) (2010).

free-ride on these mandates, thereby reducing implementation costs.

Establishing information storage requirements through public law is challenging. Governmentally specified mandates risk being overly costly, rapidly obsolete, or poorly tailored.[362] Deference to private sector best practices, though, risks insufficient precautions. Firms in the same industry may be willing to accept risks, such as cyberattacks, if those risks would cripple all competitors equally. For example, firms often fail to take adequate data security measures when they face little threat of liability or significant reputational sanctions for data spills.[363] Thus, despite arguments that private sector precautions for cybersecurity are sufficient, this Article suggests that cybersecurity regulation of information should do three things: mandate inefficiency in storage, test, and invest.[364]

1. Mandate Inefficient Storage

First, Congress should pass cybersecurity legislation that requires information to be stored inefficiently. There are three legislative dimensions to consider: which entities should be covered, what inefficient storage means, and how to enforce the mandate. The coverage dimension of cybersecurity has been the subject of considerable controversy, primarily over what constitutes "critical infrastructure" subject to enhanced regulation.[365] The scope of such critical infrastructure has expanded greatly over time, and particularly with increasing time after the ter-

362. *See, e.g.*, Derek E. Bambauer, *Rules, Standards, and Geeks*, 5 BROOK. J. CORP. FIN. & COM. L. 49, 49 (2010) (arguing that rules, specifically in industries characterized by dynamism, tend to be either under- or over-inclusive and can be difficult to change).

363. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 925–32 (2007).

364. The need for such an regulation can be evidenced by looking to a recent cybersecurity summit in Dallas, TX. *See generally* Abigail Rabinowitz, *Protecting the Digital Economy*, EASTWEST INST. (Jan. 10, 2011), http://www.ewi.info/protecting-digital-economy (showing arguments that the private sector and the public sector have not worked together effectively to promote cybersecurity and that greater collaboration is needed).

365. *See, e.g.*, *Cybersecurity: A Review of Public and Private Efforts to Secure Our Nation's Internet Infrastructure: Hearing Before the Subcomm. on Info. Policy, Census & Nat'l Archives of the H. Comm. on Oversight & Gov't Reform*, 110th Cong. 23 (2007) (statement of Gregory C. Wilshusen, Director of Information Security Issues, GAO), *available at* http://www.gao.gov/new.items/d08212t.pdf (noting that legislation on critical infrastructure protection does not address Internet disruptions).

rorist attacks of September 11, 2001.[366] Ironically, this makes later iterations of the term less useful for cybersecurity purposes. For example, Homeland Security Presidential Directive 7, signed by President George W. Bush on December 17, 2003, sweeps in "key resources," along with critical infrastructure, as targets for increased protection, where key resources include national monuments and parks.[367] Yellowstone National Park is unlikely to hold sufficiently critical information to be worthy of enhanced protection. Cybersecurity legislation could borrow more specific definitions of what constitutes critical infrastructure in the United States in defining coverage, such as that contained in President Bush's executive order establishing the Office of Homeland Security in 2001.[368] Section 3(e) of that executive order sets out a specific list of critical infrastructure that the new office is charged with protecting against the consequences of terrorist attacks.[369] This list of relevant industries and economic sectors makes for a useful initial coverage set for information inefficiency regulation.

An alternative approach to coverage, which would be more precise but less accurate, would be to impose information inefficiency requirements on entities covered by existing legal requirements to perform data retention. This requirement would be both over-inclusive (medical device manufacturers are not necessarily vital to economic functioning)[370] and under-inclusive (not all ISPs would necessarily be covered).[371] Howev-

366. *See, e.g.*, JOHN MOTEFF & PAUL PARFOMAK, CONG. RESEARCH SERV., RL32631, CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION 6–7 (2004), *available at* http://www.fas.org/sgp/crs/RL32631.pdf (describing the USA PATRIOT Act, which defines "critical infrastructure").

367. *Id.* at 9–10; *see also* 6 U.S.C. § 101(9) (2006) (defining "key resources"); 42 U.S.C. § 5195c(e)(2006) (defining "critical infrastructure" as systems and assets "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact" on national security or public health).

368. *See generally* Establishing the Office of Homeland Security and the Homeland Security Council, Exec. Order No. 13228, 66 Fed. Reg. 51,813 (Oct. 8, 2001).

369. *Id.* at 51,813–14.

370. *Cf. supra* note 360 and accompanying text (implying that medical device manufacturers are not vital by having shorter required data retention periods than other industries).

371. *Cf.* Jaikumar Vijayan, *DOJ Seeks Mandatory Data Retention Requirement for ISPs*, COMPUTERWORLD (Jan. 25, 2011), http://www.computerworld.com/s/article/9206379/DOJ_seeks_mandatory_data_retention_requirement_for_ISPs (exploring the current state of data retention with ISPs and noting that policy differences between entities has made lawful means of obtaining valua-

er, this approach would include entities that have implemented redundant data storage strategies already. While the new mandate would increase the cost of existing strategies, the cost differences would be incremental, rather than incorporating the greater expenses of initial implementation.

The second critical legislative question is what inefficiency means—in other words, what scope of information must be stored inefficiently? Organizations already evaluate this issue when implementing a data backup strategy.[372] Retaining greater volumes of data longitudinally allows an organization to recover information farther back in time but boosts storage costs and may generate greater legal exposure as more data can be discovered in litigation.[373] For regulators, this tradeoff is made more complicated by the diversity of information needs across sectors. Health service providers, for example, may need to maintain data longer than other organizations. While patients may interact with their doctors infrequently, their complete medical histories are vital to proper treatment. Retail businesses may have less need for historical data as customers and customer needs change more rapidly. Regulators could either set a uniform requirement for data inefficiency or tailor rules to each industry.[374] Targeted rules align costs most closely with benefits, but they also involve greater administrative costs in design and enforcement, and invite strategic behavior by regulated entities.[375]

ble evidence ineffective in certain instances, thus suggesting that future laws may have similar results).

372. *See, e.g.*, W. CURTIS PRESTON, BACKUP & RECOVERY 14 (2007) (noting the "need to balance the cost of a particular backup implementation against the projected monetary loss of the outage from which it protects you").

373. *See, e.g.*, Laurie Miller et al., *Document Retention Policies Revisited*, NIXON PEABODY LLP (May 27, 2003), http://www.nixonpeabody.com/linked_media/publications/CRA_05272003.pdf (acknowledging that "unnecessary document retention is prohibitively expensive" and can make responding to discovery requests difficult).

374. In regulating information practice in the private sector, for example, the U.S. Federal Government has opted for industry-specific policies rather than comprehensive legal rules. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500 (1995).

375. *Cf.* William Fisher III, *The Disaggregation of Intellectual Property*, 55 HARV. L. BULL. 24, 29–30 (2004), *available at* http://www.law.harvard.edu/news/bulletin/2004/summer/feature_2-1.php (discussing the relative merits of broad versus industry-specific rules for intellectual property and arguing that disaggregation in rules is superior since industries vary in the amount of legal incentives necessary to spur innovation and compliance).

Determining the optimal period for retaining information in an inefficient fashion, what information should be included, and whether the retention period should vary by entity or industry are difficult empirical questions that require balancing costs and benefits beyond the scope of this Article. Yet all policy debates require a starting point. Accordingly, I propose the following rule, to apply to all regulated entities, as an initial requirement:

> An organization shall maintain separate and redundant information such that, within 24 hours of losing all access to its primary data store, it is able to conduct operations in its ordinary course of operations for seven consecutive business days.

Put simply, each regulated organization should store information in a way that ensures that if it loses its primary data bank, it is able to restore normal operations within a day, and to continue those operations for a week. This rule is likely to be risk-averse, or conservative, for two reasons. First, data from disasters such as the terrorist attacks of September 11, 2001, suggest that many businesses are already able to return to operations within a few days, even after major disruptions.[376] Shortening the exposure window to one day will create incremental costs, but it is not likely to be a disproportionate burden. Moreover, service level agreements (SLAs) with information service providers, such as IT outsourcing firms, often mandate recovery of full operations in even shorter time periods.[377] Verio, for example, offers storage services that provide for data recovery in two hours during normal business operations, and in four hours during after-hours periods.[378] Second, larger and more sophisticated businesses generally operate redundant data centers, allowing them to switch operations between centers in case of disruption.[379] For example, Oracle op-

376. For examples of rapid repairs to Internet connectivity following various disasters, see *supra* Part II.C.

377. *See, e.g.*, Jonathan Raku Mathiesen, *Service Level Agreements for Storage: Report and Sample Documents*, PRESTOSPACE, 14–15 (Feb. 23, 2007), http://prestospace.org/project/deliverables/D13-5.pdf (showing that a Verio storage SLA requires a restoration time of four hours or less).

378. *Id.* at 15.

379. *See, e.g.*, Rachel Melcer, *Ready to Serve*, ST. LOUIS POST-DISPATCH, Jan. 9, 2008, at C1; Randall Stross, *99.999% Reliable? Don't Hold Your Breath*, N.Y. TIMES, Jan. 9, 2011, at B3 (explaining Gmail's practice of using two perfectly mirrored live copies in addition to its backup copies stored offline *But see* Joseph Menn & Michelle Quinn, *Power Outage Shuts Down Websites*, L.A. TIMES, July 25, 2007, at C3 (describing data center outage that knocked e-commerce firm RedEnvelope offline after RedEnvelope discontinued redundant data centers).

erates mirrored global data centers in Texas and Colorado.[380] This implies that larger entities will not find the new information efficiency mandate unduly burdensome. Smaller entities, which are more likely to incur costs in transitioning to the new regulatory scheme, can obtain some relief under the subsidy provisions described below. Moreover, small organizations can outsource services for information inefficiency, reducing their cost burdens relative to in-house provisioning.[381]

An even more conservative rule would assume that disruptions to information will include physical as well as digital effects.[382] This rule would require organizations to create inefficiency not only for information, but also for infrastructure. This rule would read:

> An organization shall maintain separate and redundant information such that, within 24 hours of losing all access to its primary data store *and data or IT center*, it is able to conduct operations in its ordinary course of operations for seven consecutive business days. [changes italicized]

This version of the rule should be reserved (if used at all) for vital information-driven industries such as the financial and banking sectors, as its implementation costs could be significant. It mandates inefficiency in both information and information processing and may require covered entities to effectively double their IT capacity.[383] Thus, this more conservative, and costly, regulation is one that should be tailored by industry sector—the added administrative costs of determining which areas are appropriately covered is justified by the burden on those regulated.

The last issue for regulation is enforcement. To be effective, enforcement regimes must be able to detect and sanction

380. Mahesh Sharma & Ben Woodhead, *Australia on Radar as Safe Site for Oracle Data Centre*, THE AUSTRALIAN, Aug. 28, 2007, at 29.

381. For a discussion of opportunities for small firms to achieve the same benefits as large organizations by outsourcing IT functions, see Jennifer Mears, *SMBs: Outsourcing a Growth Tool*, NETWORK WORLD (Feb. 27, 2006), http://www.net-directions.com/info/.

382. For example, loss of power could jeopardize an organization's ability to use its data center. *See, e.g.*, John Holusha, *Preserving Data, and Businesses*, N.Y. TIMES, Oct. 21, 2001, at RE1.

383. *But see* Mears, *supra* note 381 (noting that although the cost of developing IT strategies can seem daunting, investing in such strategies can actually reduce an organization's expenses by defraying traditional capital investment in infrastructure and technology, thereby saving the organization money long-term).

violations predictably.[384] Enforcement of the information inefficiency rule should turn on self-certification based on testing, backed by randomized auditing of those testing procedures and results for organizations that do not use outside auditors.[385] This approach reduces enforcement costs to the public fisc by transferring a portion of the costs to the regulated entities. This approach also addresses the risk of cheating through the use of credible third parties (accounting firms for publicly traded companies) and governmental inspection (for other entities).

Determining the proper level of sanctions for violations of the rule is easy in principle but difficult in practice.[386] Setting penalties too high is problematic if the state has some error rate in determining correctly whether a violation has occurred, as firms may over-invest in precautions.[387] Setting penalties too low creates incentives for non-compliance.[388] Given these uncertainties, and information asymmetries between regulators and regulated entities, the best way to set a penalty for violators is to use market information. The regulation should require the Department of Commerce to impose a heightened fine on violators who are detected through governmental audits (which come at greater cost to the public treasury) or who have had a prior violation in the past ten years.[389] For these viola-

384. *See generally* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968) (discussing an "economic" approach to enforcing legislation); *see also* A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LITERATURE 45, 45 (2000) (presenting "the economic theory of public enforcement of law in a systematic and comprehensive way").

385. *See infra* Part V.A.2 (arguing that organizations should be required to test and certify their ability to comply with the proposed cybersecurity rules).

386. *See, e.g.*, Louis Kaplow, *The Optimal Probability and Magnitude of Fines for Acts That Definitely Are Undesirable*, 12 INT'L REV. L. & ECON. 3, 3 (1992) (noting that complete deterrence of crimes is often not desirable because of the costs of enforcement).

387. *See* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 474–75 (2004) (discussing the chilling effect on desirable acts caused by sanctions that are greater than the harm sought to be deterred).

388. *See generally* Lucian Arye Bebchuk & Louis Kaplow, *Optimal Sanctions When Individuals Are Imperfectly Informed About the Probability of Apprehension*, 21 J. LEGAL STUD. 365 (1992) (considering the problem of setting optimal sanctions when actors' information about the probability of apprehension is not perfect).

389. *Cf.* David A. Dana, *Rethinking the Puzzle of Escalating Penalties for Repeat Offenders*, 110 YALE L.J. 733, 735–40 (2001) (recognizing the historical practice of escalating penalties for repeat violators and discussing how the conventional economic model holds that "an optimal expected penalty should equal the harm [or cost] to society of the violation").

tors, there should be a two-part penalty. First, the organization must outsource its implementation of the information inefficiency rule for the next five years—and must engage a firm qualified to audit publicly traded companies in the U.S. to report on its compliance with this penalty. This part of the sanction would force the violator to turn over compliance to a service provider capable of meeting regulatory requirements. In addition, third-party monitoring should reduce recidivism at the violator's expense.[390]

Second, the organization must pay a penalty equal to 1.5 times the average annual cost of the outsourcing. The fine would remove any incentive to shirk compliance for cost reasons, as it would be less expensive simply to turn over information inefficiency operations to an outside service provider. Moreover, the fine would solve the information asymmetry problem that bedevils regulators when setting penalty levels[391] by effectively imposing a market test: the violator has incentives to find the best value in outsourcing, knowing that its bargain will also set its fine.

In addition, sanctions on repeat offenders should be made public. This would increase the bite of market-based reputational sanctions and allow consumers to select away from organizations with poor cybersecurity.[392] For example, the regulation could require that such sanctions be disclosed in securities filings, as the SEC attempted to do with publicly traded entities facing environmental liabilities.[393] Revealing organizations' failures to take adequate cybersecurity precautions would deter violations and improve market data for consumers seeking more resilient firms.

390. *See generally* Dilip Mookherjee & I.P.L. Png, *Monitoring vis-à-vis Investigation in Enforcement of Law*, 82 AM. ECON. REV. 556 (1992) (suggesting that socially optimal sanctions balance the benefits derived by offenders against the harm caused by non-offenders).

391. *See* David M. Driesen & Shubha Ghosh, *The Functions of Transaction Costs: Rethinking Transaction Cost Minimization in a World of Friction*, 47 ARIZ. L. REV. 61, 80–81 (2005) (describing the difficulty, both in terms of time and cost, that pollution regulators would face in attempting to assign non-uniform pollution-reduction obligations on facilities).

392. *See* David Charny, *Nonlegal Sanctions in Commercial Relationships*, 104 HARV. L. REV. 375, 411–12 (1990) (arguing that "reputational sanctions" correct for deficiencies in legal sanctions).

393. *See, e.g.*, Barnaby J. Feder, *New Battles Over Disclosure*, N.Y. TIMES, June 24, 1990, at F10; William Baue, *SEC Urged to Strengthen Rules Governing Corporate Disclosure of Environmental Risks*, SOCIALFUNDS (Aug. 21, 2002), http://www.socialfunds.com/news/article.cgi/911.html.

First-time violators detected through private audits who have not had a previous violation in the past decade should pay a fine equal to three-quarters of the cost of one year of outsourcing.[394] While determining the cost of outsourcing will impose some administrative expense on government regulators, the existence of a competitive information technology services market should provide reliable data at low cost. Overall, this graduated-penalty scheme would minimize both enforcement costs and incentives to avoid compliance.

Like the definition of information, the proposed requirement for inefficient data storage is purposive: it compels businesses to evaluate what information they need to operate normally after losing their usual ability to access and alter content. The proposed requirement also builds on existing practices in data backup and recovery. Indeed, the federal government's Ready Business program encourages businesses to perform data backup, including storing redundant data offsite.[395] Data inefficiency has side benefits for low-incidence, high-magnitude risks to information such as natural disasters or hacking: recovery is the same regardless of the cause of information loss. The next Section of this Article discusses verifying whether this inefficiency is sufficient.

2. Test

The second regulatory move that the U.S. should make to improve the inefficiency of information storage is to mandate that regulated entities—those required under the rules described above to keep redundant data—test whether their precautions are sufficient. Cybersecurity regulation should require each organization to test its ability to meet the demands of the recovery rule, and to certify the results. Moreover, these certifications should, after a one-year grace period following the enactment of the implementing legislation, be made public. This publicity should generate market-based and norms-based pressures on organizations to comply.[396] For publicly traded

394. The implementing legislation should bestow deference on the Department of Commerce to ascertain this cost through market information. Administrative costs could be minimized by simply allowing the Department of Commerce to take a small sampling of price data from outsourcing firms based on the violator's industry and size.

395. *Improve Cyber Security*, READY BUSINESS, http://www.ready.gov/business/protect/cybersecurity.html (last updated Apr. 26, 2011).

396. *See* Charny, *supra* note 392 (suggesting that "reputational sanctions" provide strong incentives for organizations to comply with rules).

companies, the verification process should be incorporated into the testing of internal procedures and controls required by Section 404 of the Sarbanes-Oxley Act and its implementing regulations.[397] Building cybersecurity testing into existing Sarbanes-Oxley procedures should increase the reliability of information inefficiency precautions at relatively minimal cost: the check is simply one additional thing that auditors verify.

For companies not covered by Sarbanes-Oxley, the testing requirement—while necessary to ensure that information inefficiency measures are not illusory or ineffective—would represent a potentially significant added cost. Sarbanes-Oxley's regulatory regime has itself come under criticism as unduly costly.[398] However, the added expense is justified by the cybersecurity benefits. Moreover, there are at least three responses to this objection. First, there is an existing industry of firms, particularly accounting firms, that have experience with Sarbanes-Oxley monitoring and certification.[399] While engaging a firm will create costs for an organization, competitive pressures among accounting, IT services, and related firms will constrain prices. The burden for firms does not seem likely to be significant, particularly when all entities in the same industry face roughly similar costs. For example, a survey of large enterprises in 2006 found the average cost to comply with Sarbanes-Oxley's requirements for financial controls, including auditors' fees, was $2.92 million.[400] Moreover, costs had fallen 35% from 2004, when firms were first obligated to comply.[401] Costs, then,

397. *See generally* Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Securities Act Release No. 8238, Exchange Act Release No. 47,986, Investment Company Act Release No. 26,068, 68 Fed. Reg. 36,636 (June 18, 2003), *available at* http://www.sec.gov/rules/final/33-8238.htm (establishing Sarbanes-Oxley reporting requirements).

398. *See generally* Anwer S. Ahmed et al., *How Costly Is the Sarbanes Oxley Act? Evidence on the Effects of the Act on Corporate Profitability*, 16 J. CORP. FIN. 352 (2010); James Freeman, *The Supreme Case Against Sarbanes-Oxley*, WALL ST. J. (Dec. 15, 2009), http://online.wsj.com/article/SB10001424052748704431804574539921864252380.html; *Sarbanes-Oxley Audits Too Costly, Regulator Says*, N.Y. TIMES (Sept. 20, 2006), http://www.nytimes.com/2006/09/20/business/worldbusiness/20iht-sec.2875515.html.

399. *See* Matthew J. Barrett, *Sarbanes-Oxley, Kermit the Frog, and Competition Regarding Audit Quality*, 3 J. BUS. & TECH. L. 207, 211–13 (2008) (identifying multiple tiers of firms with expertise in Sarbanes-Oxley auditing).

400. *SEC Moves to Reduce Sarbanes-Oxley Costs*, N.Y. TIMES (May 23, 2007), http://www.nytimes.com/2007/05/23/business/worldbusiness/23iht-regs.4.5843700.html (describing study by Financial Executives International).

401. *Id.*

were not only manageable, but decreasing as firms became more experienced with the regulation—as a percentage of revenues, costs were lower in 2007 than in 2006.[402] As with Sarbanes-Oxley, initial expenditures for implementing information inefficiency, and for testing those new systems, are likely to be high, but are also likely to drop with time. Moreover, much of that initial expenditure will be directly beneficial to organizations by enabling them to reduce cybersecurity risks. Second, the public subsidy described below will defray at least part of the cost that organizations must assume. Finally, either cybersecurity is a significant risk to U.S. interests or it is not.[403] Imposing cost burdens, and overcoming resistance from regulated entities, is in some sense the acid test of regulation. If the risks from a lack of cybersecurity are at all like those described in Part II, testing and reporting costs are a small price to pay. Data backups, it is said, are worthless until needed—then, they are priceless. This applies with equal force to cybersecurity.

3. Invest

Finally, legislation to implement information inefficiency should provide financial support for organizations that will face new data requirements. This is, in effect, public investment in private cybersecurity. These new technology and testing costs may particularly affect small businesses that are not publicly traded. Subsidizing initial costs, particularly for small businesses, will both increase compliance and reduce political resistance to the new regulatory scheme. The public subsidy should be gradually phased out over time, as firms absorb initial overhead costs of the new information systems, and as testing and monitoring costs fall. This method has been used in other regulatory contexts with cost burdens: companies with fewer than twenty-five workers, and average annual employee pay of less than $40,000, will receive tax credits to underwrite health insurance premiums under the new health care legislation; the subsidy lasts for up to two years for each business.[404] Along similar lines, small businesses pay lower fees to the Food and Drug Administration for required medical device product re-

402. *FEI Survey: Average 2007 SOX Compliance Cost $1.7 Million*, FEI, (Apr. 30, 2008), http://fei.mediaroom.com/index.php?s=43&item=204.

403. *Cf.* MUELLER, *supra* note 27, at 179–80 (discussing transformation of cybersecurity into a national security issue).

404. Courtney Rubin, *What Health Care Reform Means for Your Business*, INC. (Mar. 22, 2010), http://www.inc.com/news/articles/2010/03/health-care-reform-and-small-business.html.

views.[405] Spending tax revenues to support compliance costs is preferable to exempting small businesses from the cybersecurity requirements, which is another common approach to reducing regulatory burdens. (Congress and the SEC faced significant pressure, for example, to exempt small businesses from the Sarbanes-Oxley requirements,[406] and companies with fewer than fifty employees are exempt from offering their workers health insurance under the new health care legislation.[407] Similarly, small businesses are exempt, under certain conditions, from registering under the Securities Act of 1934 when offering securities.[408]) Thus, Congress should offer transitional support for organizations, particularly small ones, while they work to come into compliance with the information inefficiency requirements of cybersecurity legislation.

There are at least two ways that Congress could invest in organizations' creation of inefficient data storage. First, implementing legislation could offer a tax credit to regulated entities.[409] If Congress considered it important to ensure predictability of tax expenditures on this aspect of cybersecurity, it could either set a maximum total payment, as with tax credits for purchases of fuel-efficient hybrid cars,[410] or it could combine a cap on per-entity deductions with a more limited scope of eligibility. Second, legislation could require entities facing the new requirements to apply for grants that would cover part or all of their expenditures. For example, the economic stimulus legislation of 2009 created a similar funding system for broad-

405. *PMA Review Fees*, U.S. FOOD AND DRUG ADMIN., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketApprovalPMA/UCM048161.htm (last updated Sept. 13, 2011).

406. *See SEC Moves to Reduce Sarbanes-Oxley Costs*, *supra* note 400.

407. Rubin, *supra* note 404.

408. 17 C.F.R. §§ 230.501 to .508 (2011) ("Regulation D").

409. The federal government uses a similar method to encourage provision of employer-based health insurance: employer premiums are excluded from employees' taxable income. *See* BOB LYKE, CONG. RESEARCH SERV., RL 34767, THE TAX EXCLUSION FOR EMPLOYER-PROVIDED HEALTH INSURANCE: POLICY ISSUES REGARDING THE REPEAL DEBATE 9–11 (2008), *available at* http://www.allhealth.org/BriefingMaterials/RL34767-1359.pdf.

410. The credit is phased out based on the number of cars sold by each qualifying manufacturer. *See Qualified Hybrid Vehicles*, INTERNAL REVENUE SERV., http://www.irs.gov/businesses/corporations/article/0,,id=203122,00.html (last updated Aug. 25, 2011).

band deployment projects.[411] The grant system would impose higher administrative costs than a tax credit, but in return could achieve greater targeting of funding and greater cost predictability.

Cybersecurity regulation should thus require entities with sufficiently important functions to store information inefficiently by mandating that they be capable of operating for a week on redundant data, by having those organizations test their abilities to do so, and by subsidizing on a short-term basis their investments in inefficiency. The next Section describes the second component of the proposed regulation: bolstering the positive aspects of access and alteration through inefficiency in network connections.

B. OVERLAPPING STRANDS

Don't become Egypt.

This message is a succinct summary of the information-based framework's second suggestion, which is to increase the inefficiency of network connections in the United States. During the popular uprising against the government of President Hosni Mubarak in early 2011, activists used Web-based methods such as e-mail, Twitter, and Facebook to plan demonstrations and to exchange information.[412] Egypt's government reacted with the Internet equivalent of the death penalty: it severed connections from Egyptian ISPs to the international network.[413] There are two accounts of how Mubarak's government took Egypt offline. In one, the government cut data links to the outside world not via clever technical means, but with phone calls to Egypt's five major ISPs, which provide routing to the wider Internet.[414] In fifteen minutes on January 27, 2011, Egypt's ISPs withdrew BGP (Border Gateway Protocol) from routing tables, leaving no paths by which data could reach users inside the country.[415] In the second, the key work was performed by the country's Communications Ministry, which shut

411. *See Program Information*, NAT'L TELECOMM. & INFO. ADMIN., http://www2.ntia.doc.gov/information (last visited Nov. 7, 2011) (describing broadband grant program under American Recovery and Reinvestment Act of 2009).

412. *Egypt Protests: Anti-Mubarak Demonstrators Arrested*, BBC NEWS (Jan. 26, 2011), http://www.bbc.co.uk/news/world-africa-12289475.

413. Matt Richtel, *Egypt Halts Most Internet and Cell Service, and Scale of Shutdown Surprises Experts*, N.Y. TIMES, Jan. 29, 2011, at A13.

414. James Cowie, *Egypt Leaves the Internet*, RENESYS (Jan. 27, 2011), http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

415. *Id.*

down Egypt's Internet Exchange Point (IXP) in Cairo, blocking data flow across the digital border.[416] The remaining links were cut by ISPs on orders from the Egyptian internal security service.[417] It helped considerably that Egypt was governed by an authoritarian regime that could deploy state pressure against ISP operators, and shut down the key IXP, with few checks.[418] The most important characteristic that let Mubarak's government make the Internet go dark for Egyptians, though, is that there were only a handful of choke points that it needed to control to shut down connectivity. Five phone calls—or one flipped switch in a data center—knocked Egypt off-line.[419] Egypt is a cautionary tale for cybersecurity efforts. Having a few points of failure where the network is vulnerable to disruption greatly increases the threat to information. Widely distributed, redundant data is of little value if the pathways to it are cut.

Ironically, influential voices in the current cybersecurity dialogue actually favor re-designing U.S. networks to look precisely like Egypt's topology. Indeed, the U.S. Department of Defense is moving to reduce the number of Internet connections between its NIRPNET network (used to share sensitive, but unclassified, information) and the wider Internet.[420] Clarke and Knake argue for creating break points in America's connectivity to the wider Internet, allowing the U.S. to raise the digital drawbridge in case of an attack.[421] But this tactic did not save Hosni Mubarak, and it would not save America, either. Data could still travel within U.S. networks—all an attacker would need would be access to computers located within American borders, such as via botnet.[422] Moreover, the U.S. is arguably the country with the greatest dependency on information flow across the Internet.[423] Breaking connections with the rest of the world might inflict more damage than it prevented. Even if sui-

416. Ryan Singel, *Report: Egypt Shut Down Net with Big Switch, Not Phone Calls*, WIRED (Feb. 10, 2011), http://www.wired.com/threatlevel/2011/02/egypt-off-switch/. An Internet Exchange Point is a location on the network where data is sorted into that destined for international endpoints and that destined for domestic ones. *Id.*

417. *Id.*

418. *Internet Filtering in Egypt*, OPENNET INITIATIVE (Aug. 6, 2009), http://opennet.net/research/profiles/Egypt.

419. *Id.*

420. CLARKE & KNAKE, *supra* note 23, at 171.

421. *Id.* at 272–76.

422. Clarke and Knake concede as much. *Id.* at 209.

423. *Id.* at xiii.

cide is preferable to homicide, the body still dies. Finally, such a change in network layout would be surpassingly expensive. Consolidating connections to foreign networks would require private companies to give up valuable infrastructure, and would raise hard questions regarding which entities should retain connectivity. In short, America should not envy Egypt's network.

The information-focused theory suggests that Internet connectivity should be inefficient—it should be redundant, running over different types of networks in different physical and logical locations, under the control of different operators. Data should be capable of flowing across multiple networks, connected at multiple points that are physically and logically independent. The United States has a built-in advantage regarding inefficiency. Unlike countries such as China[424] and Saudi Arabia,[425] which designed their network topologies from scratch to enable concentrated points of control[426] where methods such as filtering could be applied, America's networks grew chaotically and organically, based on market demand and organizational self-interest. However, U.S. connectivity still evinces a number of locations that could act as choke points.[427] Sean Gorman, a graduate student at George Mason University, mapped the major fiber optic cable routes in the U.S. for his Ph.D. dissertation; there are locations where physical disruption could have significant repercussions for Internet connectivity.[428] (Indeed, Gorman has separately noted that a severed cable in 1990 shut down all three of New York City's airports, along with the New York Mercantile Exchange.)[429] Moreover, the ongoing deployment of high-capacity fiber worsens the problem, as network providers consolidate onto those cables and reduce redundancy for cost reasons.[430] And fiber optic

424. *See, e.g.*, GREG WALTON, CHINA'S GOLDEN SHIELD 9 (2001).

425. *Internet Filtering in Saudi Arabia in 2006–2007*, OPENNET INITIATIVE (2007), http://opennet.net/studies/saudiarabia2007.

426. *See generally* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003) (discussing transit points in regards to Internet regulation).

427. *See, e.g.*, SEAN P. GORMAN, NETWORKS, SECURITY AND COMPLEXITY 11–27 (2005) (discussing various threats to connectivity such as power failures in certain geographic areas).

428. Laura Blumenfeld, *Dissertation Could Be Security Threat*, WASH. POST, July 8, 2003, at A1.

429. Sean P. Gorman, Is There a Cybersecurity Threat to National Security: An Interpretive Analysis (unpublished manuscript), *available at* http://gembinski.com/interactive/GMU/research/Cyber_threat_paper.pdf.

430. *Id.* at 4.

cables, if damaged, must be repaired manually in a time-consuming process.[431]

The physical connections along which Internet data travel tend to be co-located with transportation routes such as rail lines and highways; damage to the roads or tracks could also cut network connections.[432] These routes themselves may have significant bottlenecks.[433] Inefficient connections may be particularly scarce in urban areas,[434] where constraints on physical location (such as the need to share utility poles, or conduits running beneath streets) may press providers to consolidate physical connectivity. And history matters: it is up to ten times as expensive to retrofit connectivity channels beneath roads as it is to install them during initial construction.[435] Thus, it is particularly helpful to have inefficiency in physical modes of connectivity.

This is an area where the United States faces an infrastructure challenge. Most customers—both residential and business—are served by, at most, two broadband network providers: their local telephone service provider (offering DSL), and their local cable company.[436] Both modalities generally rely on wired connections, and those wired connections are often co-

431. *See, e.g.*, Lindsay Goldwert, *How Do You Fix an Undersea Cable?*, SLATE (Jan. 8, 2007), http://www.slate.com/id/2156987/.

432. Mitchell L. Moss & Anthony M. Townsend, *The Internet Backbone and the American Metropolis*, 16 INFO. SOC'Y 35, 39 (2000).

433. The intercontinental railroad system that crosses the U.S. depends on a single switching yard located outside Cincinnati, and there are only six railroad bridges across the Mississippi and Missouri rivers large enough to carry commercial traffic. Robert D. Steele, *Takedown: Targets, Tools, and Technology*, *in* CHALLENGING THE UNITED STATES SYMMETRICALLY AND ASYMMETRICALLY: CAN AMERICA BE DEFEATED? 123, 124–25 (Lloyd J. Matthews ed., 1998).

434. *See* Moss & Townsend, *supra* note 432, at 41–46.

435. Ryan Singel, *Senators Introduce "Run the Tubes Under The Highway" Bill*, WIRED (June 15, 2009), http://www.wired.com/epicenter/2009/06/senators-introduce-run-the-tubes-under-the-highway-bill/.

436. FED. COMMC'NS COMM'N, HIGH-SPEED SERVICES FOR INTERNET ACCESS: STATUS AS OF DECEMBER 31, 2008, at 3, 11 (2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296239A1.pdf (finding that cable and DSL connections comprised 77% of broadband access, and that mobile wireless devices, such as smartphones, comprised 18%). *See generally* BERKMAN CTR. FOR INTERNET & SOC'Y, NEXT GENERATION CONNECTIVITY: A REVIEW OF BROADBAND INTERNET TRANSITIONS AND POLICY FROM AROUND THE WORLD 82–83 (2009), *available at* http://www.fcc.gov/stage/pdf/Berkman_Center_Broadband_Study_13Oct09.pdf (identifying the historical trends in American telecommunications expansion).

located for significant portions of their runs.[437] Building inefficiency into the physical pathways, via diversity, creates resilience in case of disruptions, and more rapid recovery from service interruptions. For example, when a backhoe operator severed a fiber optic cable in the Yukon, Internet service was dramatically slowed.[438] The network provider, Northwestel, was able to maintain some connectivity, however, because it had maintained a set of radio towers as a back-up system.[439] When Egypt's government cut Internet connections to the rest of the world, some users were able to maintain access by using satellite-based services.[440] A group of hackers used fax machines to spread information about international dial-up Internet access to Libyans when Libya's former government regime cut standard Internet access during anti-government demonstrations.[441] As described above, the attacks of September 11, 2001 severed Internet connections even for firms that had purchased redundant connections—but whose multiple Internet pathways flowed through the same physical space in Manhattan.[442] Thus, it would be useful to increase cybersecurity by causing network service providers to build out additional capacity and connections.

Regulating America's network providers, however, has historically been challenging. Firms offering Internet access and transport have been quick to contest attempts to constrain their behavior in contexts from network neutrality,[443] to common carriage requirements,[444] to content filtering.[445] Moreover,

437. *See generally* Kevin Poulsen, *The Backhoe: A Real Cyberthreat*, WIRED (Jan. 19, 2006), http://www.wired.com/science/discoveries/news/2006/01/70040?currentPage=all (describing the sustained damage potential from severed fiber-optics).

438. Tristin Hopper, *Backhoe Severs Information Superhighway*, YUKON NEWS (June 12, 2009), http://www.yukon-news.com/news/13179/. While this incident took place in Canada, the problem is precisely analogous for the United States.

439. *Id.*

440. James Glanz & John Markoff, *Egypt's Autocracy Found Internet's 'Off' Switch*, N.Y. TIMES, Feb. 16, 2011, at A1.

441. Sean Bonner, *Operation "Libya White Fax"*, BOINGBOING (Feb. 21, 2011, 10:52 AM), http://www.boingboing.net/2011/02/21/operation-libya-whit.html.

442. *See supra* Part II.C.

443. Comcast v. Fed. Commc'ns Comm'n, 600 F.3d 642, 644–45 (D.C. Cir. 2010).

444. Nat'l Cable & Telecomm'ns Ass'n v. Brand X Internet Servs., 545 U.S. 967, 973–80 (2005).

445. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 610–11 (E.D. Pa. 2004).

the vast majority of network infrastructure in the U.S. is privately owned.[446] Network providers have topologies and redundancy levels that meet (but rarely exceed) their customers' demands—routing data is a competitive market, and excess capacity creates needless cost. Most, if not all, peering agreements between network service providers operate on a best-efforts model: there are no service-level agreements that promise a certain measure of reliability or access.[447] Accordingly, there are fewer contractual or competitive forces driving investment in guaranteed connectivity. Telecommunications companies were chastened by the industry's financial crisis in the early years of the twenty-first century, which was generated primarily by overinvestment in network capacity.[448] Thus, creating inefficiency in network connectivity requires private entities to take on investments in capacity that cannot be cost-justified as investments.[449] Governmental regulation that forces providers to build out their networks without concomitant demand is likely to be resisted fiercely.

Regulation to increase the inefficiency of Internet connections in the U.S. should therefore do three things: subsidize interconnection, mandate connectivity during disputes, and expand last-resort options.

1. Subsidize

Put simply, if the U.S. government believes network providers should deliberately incur the costs of inefficient connectivity, it should pay for that belief. Routing data is a competitive industry, and firms strive to match build-out to demand, and to projected demand.[450] Requiring network providers to

446. NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 17, at 2.

447. Michael Kende, *The Digital Handshake: Connecting Internet Backbones* 6 (Fed. Commc'ns Comm'n, Office of Plans & Policy Working Paper No. 32, 2000), *available at* http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp32.pdf; *see, e.g.*, *Verizon Business Policy for Settlement-Free Interconnection with Internet Networks,* VERIZON, http://www.verizonbusiness.com/terms/peering/ (last visited Nov. 7, 2011).

448. ELI M. NOAM, MEDIA OWNERSHIP AND CONCENTRATION IN AMERICA 268–69 (2009).

449. *See generally* Poulsen, *supra* note 437 (noting Sprint decided against physically separated data paths based on cost).

450. *See, e.g.*, GAO, GAO-04-241, WIRE-BASED COMPETITION BENEFITED CONSUMERS IN SELECTED MARKETS 1, 12–17 (2004), *available at* http://www.gao.gov/new.items/d04241.pdf; Howard A. Shelanski, *Adjusting Regulation to Competition: Toward a New Model for U.S. Telecommunications Policy*, 24 YALE J. ON REG. 55, 69–76 (2007).

carry excess capacity to ensure resilience in the face of a cyberattack will increase costs. There are two ways to cover these costs: by forcing ISPs to pass them through to customers, and by paying for them directly. The former is a tax, and the latter is a subsidy. The inefficient network connectivity is intended to benefit all American users (and perhaps all users generally) attached to the Internet—it constitutes a benefit conferred by providers onto users who are not their customers, and therefore is a classic positive externality.[451] Funding inefficient connections through a tax effectively causes an ISP's customers to subsidize Internet users generally and non-customers in particular. This may be acceptable if all users pay the tax at some point (because all users are customers of at least one ISP), but it seems more efficient to use a governmental subsidy. With a subsidy, administrative costs are lower: the State avoids the expense of collecting the tax from ISP customers, as it must incur the costs of funding additional connectivity under either system. This approach also has the benefit of being more politically acceptable to network providers, who might otherwise oppose this change, although it does increase the financial burden on the public.

Fortunately, the Obama administration has already shown a willingness to fund connectivity through the Department of Commerce's Broadband Technology Opportunities Program (BTOP), which distributed roughly $3.5 billion to build 120,000 miles of broadband network to connect underserved communities.[452] BTOP grew out of the American Recovery and Reinvestment Act of 2009, which used tax revenues to fund public infrastructure as an economic stimulus.[453] Investing in redundant connectivity is not merely a way to create additional Internet infrastructure, it is also protection—insurance—against cybersecurity risks. Government is often the insurer of last resort for high-magnitude, low-incidence risks such as terrorism, floods, and natural disasters, and so public spending seems justified here.[454]

451. *See* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 488–91 (1998).

452. NAT'L TELECOMMS. & INFO. ADMIN., BROADBAND TECHNOLOGY OPPORTUNITIES PROGRAM: OVERVIEW OF GRANT AWARDS 3–4 (2010), *available at* http://ntia.doc.gov/files/ntia/publications/ntia_report_on_btop_12142010_0.pdf.

453. *Id.* at 2.

454. *See, e.g.*, Michelle E. Boardman, *Known Unknowns: The Illusion of Terrorism Insurance*, 93 GEO. L.J. 783, 783 (2005); Dwight Jaffee & Thomas Russell, *Markets Under Stress: The Case of Extreme Event Insurance*, *in* ECO-

The governmental subsidy should cover three things: build-out of additional network backbone; transit for Tier 2 ISPs in cases where peering is not economically feasible; and an annual grant system for Tier 3 ISPs.[455] Building additional network backbone to create redundant connections is relatively straightforward: Congress should allocate money for the National Telecommunications and Information Administration to spend. Adducing a budget figure for this spending is difficult, primarily because the size of the task is hard to scope. Maps of the Internet backbone at a physical level are fragmentary, partly due to competitive concerns among providers, and partly due to physical security concerns among providers and with the government.[456] As described above, a graduate student who produced the best such map was at significant risk of having his work classified, and his research has not been made publicly available. Thus, the first step that Congress should take is to fund NTIA to undertake a study to map the Internet backbone in the United States, including interconnection points, physical location, type of physical connectivity (such as fiber optic cable), ownership, and average and peak traffic data. The study should also attempt to estimate cost for major backbone segments: how much would it cost to create a redundant connection in a separate physical location? To overcome provider reluctance to share competitive data, legislation authorizing the study should limit public dissemination to aggregate data, perhaps at the regional level, so as to obscure cost differences between providers.[457]

Second—though perhaps most important—the subsidies should defray, in whole or in large part, the cost of additional connectivity for Tier 2 ISPs. Tier 2 network providers are those that are too small to route data solely through peering arrangements; they must pay for access to at least some routes or networks.[458] The inefficiency goal for Tier 2 providers is to elim-

NOMICS FOR AN IMPERFECT WORLD: ESSAYS IN HONOR OF JOSEPH E. STIGLITZ 35, 49 (Richard Arnott et al., eds., 2003); *Warming Cited for $900 Billion Insurance Risk*, MSNBC (Apr. 20, 2007), http://www.msnbc.msn.com/id/18228964/ns/us_news-environment/.

455. On defining tiers of ISPs, see HANDBOOK OF ENTERPRISE INTEGRATION 66–67 (Mostafa Hashem Sherif ed., 2010).

456. *See supra* notes 427–30 and accompanying text.

457. *Cf.* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. (forthcoming 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749 (discussing data protection and anonymization techniques).

458. Peering is a business arrangement between ISPs, who agree to carry each other's traffic without remuneration. *See* William B. Norton, Internet

inate single points of failure and, optimally, to have the capability to route traffic (even at degraded speeds) even if connections to upstream Tier 1 ISPs were severed. Tier 2 providers should be encouraged to peer with one another. Where peering is not economically feasible, public funding should cover transit costs to ensure that each Tier 2 ISP can peer, and thereby route data in the event of loss of all upstream connectivity to Tier 1 providers. To prevent Tier 2 providers from engaging in strategic behavior, such as charging other similarly situated providers for transit instead of peering with them, the funding formula should use an offset: each provider would receive funds to cover their transit costs, net of what they charge to other Tier 2 ISPs. This approach would also helpfully provide greater subsidies to smaller providers.

Lastly, the subsidy should cover some costs of greater connectivity, and hence greater inefficiency, for Tier 3 providers. These ISPs rarely peer, but instead purchase connectivity. Their networks may contain single points of failure, with but one source of upstream connectivity due to cost constraints.[459] While increasing inefficiency for Tier 3 ISPs seems attractive, it may not be sensible. It might be more efficient for downstream customers to instead purchase service from a Tier 2 ISP. Thus, it is not certain that dedicating funding to Tier 3 providers is desirable. A compromise solution would be for Congress to authorize a set amount for grants by NTIA to Tier 3 ISPs, along the lines of the successful BTOP program.[460] Tier 3 providers could apply for grants to cover additional connectivity, based on the number of downstream users served (with preference to larger ISPs); the level of competitive alternatives in their market (with preference to providers of last resort); and the proposal's cost-effectiveness. The funding criteria should be deliberately Darwinian: more efficient and effective Tier 3 ISPs should preferentially receive support.

Proposing additional government spending is problematic at a time of economic downturn and political concern about budget deficits. However, spending is where political rhetoric about cybersecurity risks is tested. Consider, for example, that President Obama's 2012 budget requested only $548 million in

Service Providers and Peering (Sept. 23, 2011) (unpublished manuscript), *available at* http://www.nanog.org/papers/isp.peering.doc.

459. HANDBOOK OF ENTERPRISE INTEGRATION, *supra* note 455.

460. *See supra* note 452 and accompanying text.

spending for cybersecurity research and development,[461] compared with $921 million in research project grants for the National Institute of Mental Health.[462] Precautions are likely to be relatively inexpensive. Total BTOP expenditures on broadband of $3.48 billion, for example, were only 70 % of the National Cancer Institute's budget in 2010.[463] They equal roughly 4.4% of estimated 2010 expenditures by the Department of Defense for research, development, testing, and evaluation.[464] By comparison, the federal government allocated $1 billion for federal food safety[465] and flood insurance programs[466] in 2010. While the BTOP allocation is an inexact guide for cybersecurity investment, it is representative. If cybersecurity threats are real, government should be prepared to spend to abate them. Moreover, contemporary rhetoric that paints cybersecurity risks as national security threats can help make spending more palatable, as it is politically difficult to oppose national security programs.[467]

2. Mandate Connectivity During Disputes

Second, regulation to produce inefficient connectivity should seek to preserve existing links between backbone providers. Disputes over peering arrangements—over costs of carrying traffic—are common between Tier 1 ISPs. Cogent, for example, is frequently involved in peering disputes due to its cut-rate pricing policy. Cogent became involved in tussles with

461. Patrick Thibodeau, *Obama Seeks Big Boost in Cybersecurity Spending*, COMPUTERWORLD (Feb. 15, 2011), http://www.computerworld.com/s/article/9209461/Obama_seeks_big_boost_in_cybersecurity_spending?taxonomyId=70.

462. NAT. INSTS. OF HEALTH, FY 2012 BUDGET 4, *available at* http://www.nimh.nih.gov/about/budget/cj2012.pdf.

463. NAT. INSTS. OF HEALTH, HISTORY OF CONGRESSIONAL APPROPRIATIONS, FISCAL YEARS 2000–2010, *available at* http://officeofbudget.od.nih.gov/pdfs/FY11/Approp.%20History%20by%20IC%20(FINAL).pdf (documenting NCI budget of $5.1 billion in 2010).

464. U.S. DEP'T OF DEF., FINANCIAL SUMMARY TABLES: DEPARTMENT OF DEFENSE BUDGET FOR FISCAL YEAR 2010, at 10 (2009), *available at* http://comptroller.defense.gov/defbudget/fy2010/fy2010_summary_tables_whole.pdf.

465. U.S. DEP'T OF AGRIC., FY 2010 BUDGET SUMMARY AND ANNUAL PERFORMANCE PLAN 68, *available at* http://www.obpa.usda.gov/budsum/FY10budsum.pdf.

466. CONGRESSIONAL BUDGET OFFICE, THE NATIONAL FLOOD INSURANCE PROGRAM: FACTORS AFFECTING ACTUARIAL SOUNDNESS 1–2 (Nov. 2009), *available at* http://www.cbo.gov/ftpdocs/106xx/doc10620/11-04-FloodInsurance.pdf.

467. *Cf.* GEORGE LAKOFF, DON'T THINK OF AN ELEPHANT! 58, 68 (2004) (describing how the national security metaphor has been employed to advocate for various policy goals).

AOL in 2002, Level 3 and France Telecom in 2005, Limelight Networks in 2007, and Telia in 2008.[468] In each case, Cogent or its adversary "de-peered" the other—they stopped accepting the other provider's traffic, voluntarily severing a major network connection.[469] This made it more difficult for their customers to communicate.[470] For example, Martha Stewart Living's website is hosted by Cogent, and during the company's dispute with Telia, Telia users could not reach it.[471] De-peering moves are a common means to pressure another network provider to accede to terms.[472] They are also a significant cybersecurity risk. Regulation should prohibit network providers from ceasing to carry their peers' traffic until alternative arrangements are made.

Banning de-peering could significantly alter arrangements between backbone network providers. De-peering is self-help: it forces a connecting provider to choose between negotiating and finding alternative routing. Thus, de-peering may serve a helpful dispute resolution function. However, the costs of breaking connections between backbone providers are too high from a security perspective. De-peering reduces network redundancy, and could create a window of opportunity for cyberthreats. In addition, a ban would come with two significant limitations that would make its drawbacks less potent. First, it would apply only when network providers were operating under a peering agreement—where they were exchanging roughly equal data volumes, without cost recovery. Most peering disputes involve parties of roughly equal bargaining power.[473] If providers were to opt to enter into a peering arrangement, they would do so knowing their tools for altering the bargain were more

468. Rich Miller, *Cogent Unplugs Telia in Peering Dispute*, DATA CENTER KNOWLEDGE (Mar. 16, 2008), http://www.datacenterknowledge.com/archives/2008/03/16/cogent-unplugs-telia-in-peering-dispute/.

469. *See id.*

470. *See* Rich Miller, *Peering Dispute Between Cogent, Sprint*, DATA CENTER KNOWLEDGE (Oct. 31, 2008, 9:56 AM), http://www.datacenterknowledge.com/archives/2008/10/31/peering-dispute-between-cogent-sprint/.

471. Tom Corelis, *Internet Rift Opens Over ISP Peering Dispute*, DAILY TECH (Mar. 22, 2008, 8:15 AM), http://www.dailytech.com/Internet+Rift+Opens+over+ISP+Peering+Dispute/article11199.htm.

472. *See id.* ("De-peering disputes often devolve into a game of 'chicken,' where the two companies try to completely cut off each other's traffic; the onus of response is left to whichever company has the largest customer uproar when their networks stop working and websites become inaccessible.").

473. See e.g., id. (discussing a de-peering example involving "two of the world's larger bandwidth providers").

limited than under fee-based carriage. Second, providers would be expressly permitted to initiate litigation to recover costs of traffic carried in excess of that transmitted—in short, to obtain damages as recompense. In addition, providers should be authorized, after a cooling-off period of thirty days, to seek injunctive relief in federal district court that would allow them to de-peer.[474] District courts should grant such injunctions under the standard four-part equitable analysis for preliminary injunctions, with particular attention to the public interest factor.[475] This would allow providers an exit strategy from particularly unprofitable or troublesome arrangements, after a delay sufficient to allow the other party to develop alternative routing strategies.

The limited de-peering ban would strongly push providers to maintain peering arrangements with one another by increasing the costs of exit. While this could cause ISPs to enter into peering arrangements more reluctantly, this is mitigated by peering's cost advantages for providers, who do not need to measure and bill traffic flow. Moreover, U.S. law does not hesitate to limit negotiating tactics where there are significant third-party interests at stake. President Ronald Reagan fired air traffic controllers who violated a statutory ban on striking,[476] and public safety workers such as police and firefighters are often prohibited from labor actions.[477] Thus, a party's right to renegotiate terms by withholding may be barred because of negative effects on those not at the bargaining table. While temporarily preventing ISPs from de-peering will alter negotiation dynamics, the limited cost is worth the gains in inefficiency of network paths.

3. Expand Alternatives

Lastly, regulation should seek to increase the heterogeneity of Internet connectivity, at least as a fallback measure. The goal is to promote ad hoc measures that can route data when ordinary networks are disrupted. This approach has been ex-

474. The thirty-day clock would begin when the ISP filed suit.

475. *See* Winter v. Natural Res. Def. Council, 555 U.S. 7, 25–26 (2008) (holding that the public interest favored the Navy's continued use of sonar radar over the interests of marine mammals who might be harmed).

476. Andrew Glass, *Reagan Fires 11,000 Striking Air Traffic Controllers Aug. 5, 1981*, POLITICO (Aug. 5, 2008, 4:30 AM), http://www.politico.com/news/stories/0808/12292.html.

477. WILLIAM H. HOLLEY ET AL., THE LABOR RELATIONS PROCESS 572–73 (9th ed. 2008).

plored by scholars such as Yochai Benkler, who argues that open wireless networks could substitute—at least where there is adequate density of network devices—for traditional Internet access provisioning.[478] This "spectrum commons" approach suggests a peer-production model of routing that is an inefficient yet highly flexible ad hoc solution.[479] Ironically, this goal may require government to *de*-regulate. One example is the proposal by former FCC chair Kevin Martin to relinquish control over the 700MHz spectrum band to enable open wireless broadband.[480] While Martin's proposal was not adopted,[481] it shows that government can sometimes increase Internet access diversity by giving up control.

Ad hoc solutions can be surprisingly robust. The earthquake that struck Haiti on January 12, 2010 damaged most of the country's backbone network and telecom data centers.[482] Aid groups rely heavily on Internet-based communication to coordinate efforts. NetHope, a humanitarian technology organization, identified a non-governmental organization with satellite-based Internet access, and created a patched-together mesh network linking recovery teams to the single access point.[483] NetHope's coordinator emphasized two lessons: "Wireless is where it's at [and] . . . [w]e're far better off investing in emergency preparedness . . . ."[484] Similarly, a team of researchers at the Research Centre for Disaster Resilience and Health at Australia's Flinders University created the Serval Project, which

478. Yochai Benkler, *Some Economics of Wireless Communications*, 16 HARV. J. L. & TECH. 25, 32 (2002).

479. *See* Yochai Benkler, *Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment*, 11 HARV. J. L. & TECH. 287, 293–94 (1998) (describing the spectrum commons approach).

480. *See* Service Rules for the 698-746, 747-762, and 777-792 MHz Bands, 22 FCC Rcd. 15,288, 15,558 (Aug. 17, 2007) (statement of Kevin J. Martin, Chairman, FCC), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-132A2.pdf.

481. *See* Paul Kapustka, *FCC Punts on 700 MHz Rulemaking*, GIGAOM (Apr. 25, 2007, 6:23 PM), http://gigaom.com/2007/04/25/fcc-punts-on-700-mhz-rulemaking/ (reporting a delay in adopting rules for the 700 MHz spectrum auction).

482. Todd Bishop, *How Haiti Got the Internet Back, With Help From a Guy in Seattle*, TECHFLASH (May 14, 2010, 9:19 AM), http://www.techflash.com/seattle/2010/05/how_haiti_got_back_online_with_help_from_former_microsoft_exec.html.

483. *Id.*

484. *Id.*

links mobile phone handsets into a local wi-fi network.[485] Tests of Serval have shown that each handset can act as a router at a distance of up to several hundred meters.[486] Engineers from the Massachusetts Institute of Technology have developed FabFi, an ad hoc mesh wireless network that builds repeater stations for around $60, made from chicken wire and locally available materials, and that provides broadband Internet access over an area with a six kilometer radius.[487]

An additional option would be for government itself to provide routing paths that are less dependent on wired networks. Various cities and municipalities have experimented with "muni wi-fi" in the past several years, but most attempts foundered under cost pressures[488] and telecommunications industry resistance.[489] However, municipal wi-fi, even in paid form or as a public-private partnership, offers significant positive cybersecurity externalities. It can serve as a fallback if commercial providers experience disruption. The experience of Minneapolis after the collapse of the city's I-35 bridge offers an example. The city had entered a partnership with US Internet, an ISP that eventually built a $20 million wireless network covering 95% of Minneapolis.[490] At the time of the collapse, US Internet had deployed a small test-network near the bridge.[491] When emergency responders overloaded the local mobile phone net-

485. Lin Edwards, *New Project Enables Mobile Phone Use in Areas with No Reception*, PHYSORG.COM (July 14, 2010), http://www.physorg.com/news198298057.html.

486. *Id.*

487. Sebastian Anthony, *Afghanistan's DIY Internet Brings the Web to War-Torn Towns*, EXTREMETECH (June 22, 2011, 8:36 AM), http://www.extremetech.com/internet/87496-afganistans-diy-internet-brings-the-web-to-citizens-without-roads-and-water.

488. *See* Tim Wu, *Where's My Free Wi-Fi?*, SLATE (Sept. 27, 2007, 12:53 PM), http://www.slate.com/id/2174858/pagenum/all/ (explaining that municipal wi-fi systems could not compete with private Internet-service providers).

489. *See, e.g.*, Chris Gonsalves, *Wi-Fi Flap Nixes Deal*, EWEEK, Dec. 12, 2005, at 28, *available at* http://www.eweek.com/c/a/Mobile-and-Wireless/Muni-WiFi-Flap-Nixes-Deal-in-New-Orleans/; Wayne Hanson, *Pennsylvania Municipalities Have One Year to Develop WiFi Networks*, GOV. TECH. (Dec. 1, 2004), http://www.govtech.com/e-government/Pennsylvania-Municipalities-Have-One-Year-to.html. *See generally* Hannibal Travis, *Wi-Fi Everywhere: Universal Broadband Access as Antitrust and Telecommunications Policy*, 55 AM. U. L. REV. 1697, 1726–63 (2006) (discussing how broadband deregulation contributed to the creation of broadband monopolies and duopolies).

490. Russell Nichols, *How to Make Municipal Wi-Fi Work*, DIGITAL COMMUNITIES (Jan. 12, 2010), http://www.digitalcommunities.com/articles/How-to-Make-Municipal-Wi-Fi-Work.html.

491. *Id.*

work with traffic, US Internet made its wireless network available for free, enabling emergency services to coordinate more quickly and efficiently.[492] Having governmental networks carry traffic in the event of disruption is a symbolic return to the Internet's inception, when the network backbone was government-owned and operated.[493] Cybersecurity considerations make the prospect worth exploring again.

Inefficient connectivity is a critical component of cybersecurity. Maintaining positive access and alteration requires that users be able to reach, and interact with, information via multiple pathways. Yet, competitive pressures in the telecommunications industry push in precisely the opposite direction: towards consolidation of routes. Regulatory efforts should thus subsidize some connectivity directly, require ISPs who peer to continue peering during disputes, and expand options for carriers of last resort. As the next Section notes, while these measures will greatly augment cybersecurity's positive aspects, they require tradeoffs.

C. SCYLLA AND CHARYBDIS

Cybersecurity requires hard choices. Like Odysseus confronting the mythical Greek sea monsters of Scylla and Charybdis, avoiding one peril risks another. The tradeoffs in cybersecurity are between the positive and negative ranges of access and alteration. Storing information in more locations, with more pathways to it, increases not only the probability that authorized users will engage with it, but that unauthorized ones will also do so. This inverse relationship is not inevitable, but it is likely, particularly when cost considerations are added.

Inefficiency does not necessarily increase the risk of negative access or alteration. Organizations could reduce both types of cybersecurity threats by storing data partially and heterogeneously. This protects information analogously to how the bibliophiles in Ray Bradbury's novel *Fahrenheit 451* preserve books in a world where they are banned and subject to destruction.[494] Guy Montag, the fireman protagonist, has memorized the Book of Ecclesiastes.[495] His compatriots have committed

492. *Id.*

493. *See* MILTON MUELLER, RULING THE ROOT 74–75 (2004) (describing the pre-Internet network operated by the U.S. Defense Department that connected research scientists in university, military, and industrial sites).

494. RAY BRADBURY, FAHRENHEIT 451, at 35–40 (1st ed. 1953).

495. *Id.* at 150.

other chapters to memory.[496] No single person has memorized the entire Bible, so no single death can delete it from human knowledge—and, analogously, no single capture provides an attacker with the whole book.[497] An inefficiency approach with partial storage breaks information into pieces that are stored in multiple locations.[498] Consider, for example, an organization with four information repositories. The organization can split its data into quarters (A, B, C, and D), and store them with one quarter per location:

Location 1: A	**Location 2:** B
Location 3: C	**Location 4:** D

It can also achieve greater inefficiency, and hence easier recovery, at the cost of doubling its storage requirements, with two quarters per location:

Location 1: A, B	**Location 2:** B, C
Location 3: C, D	**Location 4:** D, A

A cyberthreat must compromise three of four locations to reassemble the entirety of the data (although the organization must also draw information from three places to recover its data).

An additional way to mitigate inefficiency's risks of unauthorized access and alteration is to store information heterogeneously, using multiple operating systems, applications, hardware, and encryption. A vulnerability in one operating system or application thus could expose part of the information, but not all of it. Thus, heterogeneity immunizes inefficient storage from a single attack vector in the way that mixed crop agriculture protects against devastation by a single pest or parasite.[499]

However, heterogeneity costs more. Most organizations standardize on a single operating system and application plat-

496. *Id.* at 153.

497. *Cf. id.* at 151 (explaining that each book of the Gospels is committed to memory by different individuals).

498. BitTorrent functions similarly. *See* Loewenstern, *supra* note 310.

499. Sandra Díaz et al., *Biodiversity Regulation of Ecosystem Services*, *in* 1 ECOSYSTEMS AND HUMAN WELL-BEING 297, 317 (Rashid Hassan et al. eds., 2005).

form—their servers run Windows or Linux, but not both.[500] Maintaining multiple variants of each type of program increases the expense and complexity of IT infrastructure.[501] Even if security efforts are effective, they may appear unnecessary—observers may conclude that threats were overstated, rather than mitigated. Heterogeneity can be helpful, but it is costly.

This Article's proposed inefficiency-based solutions would improve authorized users' abilities to access and alter information. However, there are likely to be tradeoffs between improving cybersecurity's positive aspects, and improving its negative ones. Future work will explore cybersecurity's negative aspects. The next Part argues that an information-oriented theory is vital not only to improving security, but also to preventing a fundamental shift in America's attitude towards open communication on the Internet.

V. THE STAKES: RE-FIGHTING OLD WARS

The stakes at issue in which theoretical model we choose for cybersecurity are considerable. The Internet's current core design permits open, anonymous communication by default—an architectural choice reflecting key American normative commitments.[502] Cybersecurity risks, though, increasingly drive demands for reform, especially when posed as threats to U.S. national security.[503] If conventional approaches, with their emphasis on ascertaining the identity and intent of those creating such threats, hold sway, the U.S. is likely to shift its emphasis from protecting open communication to prioritizing authentication. The consequences would be profound, and harmful. They would include not only harm to the Internet's generative capacity, but even more importantly to America's role in checking attempts to quell on-line expression, particularly by authoritarian states such as China and Russia.[504]

500. *See, e.g.*, Tom Duffy, *Standard Issue*, NETWORK WORLD, Apr. 3, 2000, at 76 (discussing the benefits of system standardization).

501. *See, e.g.*, M. GORDON HUNTER, CONTEMPORARY CHIEF INFORMATION OFFICERS: MANAGEMENT EXPERIENCES 61 (2007) (describing how standardization reduced time spent on maintenance and helped control IT costs).

502. Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 520 (2002).

503. *See* Dycus, *supra* note 22, at 155–56 ("The very future of the Republic may depend on our ability not only to protect ourselves from enemies armed with cyber weapons, but also to use such weapons wisely ourselves.").

504. *See* Viktor Mayer-Schönberger & Malte Ziewitz, *Jefferson Rebuffed: The United States and the Future of Internet Governance*, 8 COLUM. SCI. &

These perils underscore the importance of which theory we adopt to deal with cyber-risks.

The struggle over cybersecurity recapitulates the definitional battles of the early Internet boom, which pitted cyber-exceptionalists[505] against cyber-realists.[506] Although the cyber-realists won that debate, the cyber-exceptionalists had a critical insight: the Internet is more resistant to control than other communication modalities—in its current form.[507] U.S. hegemony over key aspects of Internet architecture has maintained this implicit preference for free communication over gate keeping, even in the face of dogged criticism and opposition.[508]

This default freedom to communicate, though, is a relic of the Internet's history. The core protocols were designed primarily by American computer scientists and engineers. It is no accident that the Internet's architecture embodies to a considerable degree the American constitution's preference and protections for free expression and access to information.[509] The default position of American constitutional jurisprudence, and of the Internet's design, is to permit communication, including

TECH. L. REV. 188, 203–04 (2007) (explaining the U.S. opposed the internationalization of Internet governance, in part, because it would give nations like China an opportunity to restrict open communication).

505. *See generally* David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (arguing that new rules would emerge to govern the Internet that diverge from the traditional rules of the physical world).

506. *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? (2006) (arguing that the Internet will be shaped by traditional principles of governance and politics within territorial nations).

507. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 514–22 (1999) (suggesting steps the government could take to shape the design of the Internet and increase its regulability).

508. *See generally* MUELLER, *supra* note 27, at 62–64 (discussing how the U.S. government exercises control over Internet governance by being the only sovereign to supervise the Internet Corporation for Assigned Names and Numbers (ICAAN)); Mayer-Schönberger & Ziewitz, *supra* note 504 (recounting international negotiations on Internet governance conducted at the World Summit on the Information Society).

509. *See* Reno v. ACLU, 521 U.S. 844, 885 (1997) (holding unconstitutional provisions of the Communications Decency Act of 1996 which sought to protect minors from obscene or indecent material on the Internet); MUELLER, *supra* note 493, at 265–66 ("The Internet was the epitome of Jeffersonian decentralization.").

anonymous communication.[510] Deviations from that standard require special justification, or technological mechanisms.[511]

Security fears, though, could lead America—no doubt with reluctance—to prioritize safety over freedom. Pressures to make the Internet more secure through attribution are mounting.[512] They could become irresistible if America suffers a high-profile cybersecurity incident. Security policy is often reactive. The Transportation Security Administration began screening airline passengers' shoes after Richard Reid attempted to ignite explosives stored in his sneakers on a flight.[513] After a data spill, the Los Alamos National Laboratory not only banned the use of flash drives, but filled USB ports on its workstations with super glue.[514] The USA PATRIOT act, with its smorgasbord of law enforcement measures, was passed quickly in the days following the attacks of September 11, 2001.[515] As John W. Kingdon emphasizes, when a focusing incident creates a policy window, policymakers and legislators generally opt for prepackaged measures rather than crafting responses from scratch.[516] Thus, if conventional methodologies for cybersecurity continue to dominate, the likely response to a significant cyber-incident would be to address those theories' core concern: the lack of attribution in the Internet's core design. The prepositioned solution for a cybersecurity problem that attracts major public notice, and generates demands for a fix, is to change how the Internet functions.

Such architectural changes will inevitably undercut the medium's power as a communications platform, damaging what

510. *See* Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1577–89 (2007).

511. *See* Network Working Gr, *RFC 1958—Architectural Principles of the Internet*, IETF (B. Carpenter ed., June 1996), http://www.ietf.org/rfc/rfc1958.txt.

512. *See, e.g.*, Kirsten Doyle, *Focus on Cyber War Defence,* ITWEB (Oct. 13, 2010), http://www.itweb.co.za/index.php?option=com_content&view=article&id=37739:focus-on-cyber-war-defence&catid=69&Itemid=58 (quoting Richard Clark, Chairman of Good Harbor Consulting, as suggesting the design of "another, more secure Internet").

513. Pam Belluck & Kenneth Chang, *Shoes Were a 'Homemade Bomb,' F.B.I. Agent Says*, N.Y. TIMES, Dec. 29, 2001, at B1.

514. Daniel Tynan, *Closed-Door Policy*, FED TECH (Sept. 10, 2007), http://fedtechmagazine.com/article.asp?item_id=352.

515. Pub. L. No. 107-56, 115 Stat. 272 (2001).

516. JOHN W. KINGDON, AGENDAS, ALTERNATIVES, AND PUBLIC POLICIES 165 (2003).

Jonathan Zittrain calls its "generativity."[517] This shift is similar to what Zittrain fears will occur as the result of users' security worries, driving them onto locked-down devices such as the iPad rather than open platforms such as Android.[518] However, the cybersecurity sea change will emanate from the top down, rather than bottom up; it will originate with governments (especially America's), not consumers, and hence is likely to be more resistant to alteration.

More importantly, the change in American priorities will significantly re-align stakeholder interests in Internet design. U.S. control over key Internet architecture has enabled America to resist calls by authoritarian countries to restrict free expression on-line.[519] States such as China and Russia work to control the ambit of Internet communication within their borders, particularly if it seems to threaten internal political hegemony.[520] American efforts to embed attribution into the Internet would unintentionally bolster their endeavors. Moreover, it would provide such states not only with new technological capabilities, but with rhetorical cover: disagreements would shift from whether to limit communication, to when.[521] This normative shift would weaken America's advocacy for free expression, and would align the U.S. in a partnership of convenience with countries that evince no real commitment to the promise of open communication. Such changes, and losses, represent the risk of using law reflexively to regulate cybersecurity without a theoretical orientation that guides its application.

In short, the current design of the Internet, where information routes by default and where security is pushed to the edges of the network, is a historical accident—an accident that cybersecurity concerns can remediate, to our collective detriment, if we choose the wrong solutions.

517. Zittrain, *supra* note 29, at 1980 ("Generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences."). *See generally* ZITTRAIN, *supra* note 74 (discussing the characteristics of a generative system).

518. Zittrain, *supra* note 29, at 2003.

519. *See, e.g.*, Rebecca MacKinnon, *China Calls for an End to the Internet Governance Forum*, RCONVERSATION (May 14, 2009), http://rconversation.blogs.com/rconversation/2009/05/china-calls-for-an-end-to-the-internet-governance-forum.html.

520. ACCESS CONTROLLED, *supra* note 95, at 209, 449.

521. *Cf.* Bambauer, *supra* note 275, at 384–86 (arguing countries differ based on the justification for censorship, not on whether to censor).

CONCLUSION

Preventing cyberattacks is impossible. Retaliation does not remediate them. Cybersecurity must come to grips with this reality.

This Article's information-oriented theory of cybersecurity focuses on resilience and recovery, rather than on prevention and retaliation, as conventional scholarly models do. Computer software is too complex to hope that systems can be sufficiently hardened to prevent attacks.[522] Knowing that the United States and Israel are behind the Stuxnet cyberweapon has not helped Iran's nuclear program recover ground. Understanding that their government intended to prevent them from organizing did not help Egyptian protesters communicate any more readily. In short, current approaches to cybersecurity aim at goals that are nearly impossible to achieve, and unhelpful if attained. The information-focused approach concentrates usefully on identifying, and protecting, what users seek to accomplish on-line.

We should also recognize that law is a limited tool for cybersecurity. Cyberthreats are inherently cross-border, and can be launched from anywhere with sufficient connectivity. Effective legal regulation thus requires consensus among sovereigns, whether those sovereigns are nation-states or relevant international bodies such as the United Nations. And states presently differ about what constitutes cybersecurity. Russia, for example, sees criticism of its government, which it terms "information war," as a cyberthreat.[523] Even the U.S. has mixed incentives for legal regulation: strengthening cyberdefenses could reduce America's vulnerabilities, but also its capability to mount its own attacks. Ineffective legal measures may be worse than none at all, as they could generate a false sense of security while closing the policy window for reform.[524]

Yet inefficiency holds promise for cybersecurity. It confers resilience in other contexts. Index funds for stock investing sacrifice the potential for enormous gains to protect against catastrophic losses, as Enron's employees learned painfully.[525] Er-

522. Bambauer & Day, *supra* note 62, at 1062 (discussing vulnerabilities in operating system (OS) software).

523. Tom Gjelten, *Seeing the Internet as an 'Information Weapon,'* NAT'L PUB. RADIO (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

524. *See* KINGDON, *supra* note 516, at 160 ("Policy windows open infrequently, and do not stay open long.").

525. *See* Martine Costello, *Company Stock Slams 401(k)s*, CNNMONEY (Dec.

rors in genetic replication enable adaptation to ecological changes. The results are not always desirable: BitTorrent's inefficient architecture helps downloaders evade copyright infringement liability,[526] and the HIV virus benefits from error-prone replication to evade immune system defenses.[527] But the lesson for cybersecurity is clear—inefficiency works.

The next Article in this project will take up the challenges of cybersecurity's negative aspects: preventing unauthorized access and alteration of information, and detecting when they have occurred. This Article seeks to define cybersecurity's conundrum, and to offer a path to solving it.

10, 2001, 11:59 AM), http://money.cnn.com/2001/12/10/401k/q_401k_lawsuits/ (reporting on the financial losses of Enron employees who held company stock following Enron's collapse).

526. *See* Ben Jones, *Are Private BitTorrent Trackers Safe?*, TORRENTFREAK (Mar. 27, 2007), http://torrentfreak.com/are-private-bittorrent-trackers-safe/.

527. A. Telesnitsky & S.P. Goff, *Reverse Transcriptase and the Generation of Retroviral DNA*, *in* RETROVIRUSES 121, 141 (John M. Coffin & Harold E. Varmus eds., 1997).