American University Business Law Review

Volume 2 | Issue 2 Article 1

2013

Fiddling on the Roof: Recent Developments in Cybersecurity

Melanie J. Teplinsky

Follow this and additional works at: http://digitalcommons.wcl.american.edu/aublr

 Part of the Law Commons

Recommended Citation

Teplinsky, Melanie J. "Fiddling on the Roof: Recent Developments in Cybersecurity." American University Business Law Review 2, no. 2 (2013): 225-322.

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Business Law Review by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact fbrown@wcl.american.edu.

ARTICLES

FIDDLING ON THE ROOF: RECENT DEVELOPMENTS IN CYBERSECURITY

MELANIE J. TEPLINSKY*

TABLE OF CONTENTS

* Ms. Teplinsky is an adjunct professorial lecturer at American University Washington College of Law ("WCL"). She also serves on the Advisory Board of CrowdStrike, Inc. and writes and speaks frequently on cyberlaw issues. Prior to joining WCL, Ms. Teplinsky practiced law at Steptoe & Johnson LLP, where she counseled leading financial services, telecommunications, and other multinational clients on a wide array of issues including cybersecurity, data protection, and electronic surveillance. Ms. Teplinsky is a graduate of Harvard Law School and served as a law clerk to the Honorable Judge Rya W. Zobel, U.S. District Court, District of Massachusetts. The author wishes to thank Arjun Prasad and the editorial staff of the *American University Business Law Review* for their exceptional work and gratefully acknowledges Dmitri Alperovitch and Steven Chabinsky, who have contributed significantly to the author's thinking about the future of U.S. cybersecurity policy. The author also wishes to thank her family for their forbearance as she worked on this article, especially her loving and supportive husband, Steven, and their six-year-old red-headed daughter, who missed mommy so much during the drafting of this Article that she asked mommy to "pinky promise" not to write another.

INTRODUCTION

[Y]ou might say every one of us is a fiddler on the roof trying to scratch out a pleasant, simple tune without breaking his neck.
-Fiddler on the Roof[1]

For today's CEOs and corporate boards of directors, trying to capture the benefits of new technology while tackling emerging cybersecurity challenges is a delicate balance akin to fiddling on the roof. This Article outlines recent developments in ".com" cybersecurity and their implications for corporate cybersecurity. Section I summarizes how information technologies have revolutionized the functioning of global economies, societies, and governments. Section II discusses the U.S. self-regulatory approach to ".com" cybersecurity and the long-standing challenge of securing critical infrastructure ("CI") networks. Sections III–V discuss technology trends, the cyberthreat landscape, and legislative developments affecting cybersecurity, respectively. Specifically, Section III outlines three technological trends that pose cybersecurity challenges: explosive growth in mobile technology; migration to cloud computing; and increasing pervasiveness of social networks. Section IV examines the increasingly complex global cyberthreat landscape, including the problems of cybercrime, cyberespionage, and cyberwarfare. Section V discusses recent congressional and executive action on cybersecurity, including the ongoing congressional debate over cybersecurity legislation. Finally, Sections VI and VII describe private sector cybersecurity challenges and opportunities, including the potential for the private sector to shift the long-standing ".com" cybersecurity debate in Washington toward a more holistic strategy that encompasses not only vulnerability mitigation, but also deterrence.

I. THE PROMISE AND PERIL OF CYBERSPACE

It has been said that "[c]yberspace touches practically everything and everyone."[2] With over two billion people relying on the Internet[3] for a

1. FIDDLER ON THE ROOF (United Artists 1971).

2. WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE i (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [hereinafter WHITE HOUSE, CYBERSPACE POLICY REVIEW].

3. U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1 (2011), http://www.defense.gov/news/d20110714cyber.pdf. ("From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people.").

wide variety of economic,[4] social,[5] and political interactions,[6] cyberspace—the "globally-interconnected digital information and communications infrastructure"[7]—is nothing short of essential to modern life.

Information technologies ("IT") have revolutionized the functioning of economies, societies, and governments around the globe. First, by any measure, IT has transformed the way we conduct business. IT has fundamentally changed the relationship between businesses and consumers, allowing not only for improved market differentiation and personalization of services, but also for the transformation of marketing through social media.[8] Internally, IT has driven business efficiency through the automation and/or reorganization of business processes, such as invoicing, recordkeeping, and supply chain management;[9] big data analytics;[10] and the

4. Global e-commerce sales are expected to reach $963 billion by 2013, according to Goldman Sachs projections. Don Davis, *Global e-Commerce Sales Head for the $1 Trillion Mark*, INTERNET RETAILER (Jan. 4, 2011, 3:02 PM), http://www.internetretailer.com/2011/01/04/global-e-commerce-sales-head-1-trillion-mark. *Cf.* SUCHARITA MULPURU ET AL., FORRESTER, THE ECOMMERCE JUGGERNAUT DOMINATES RETAIL 1 (2012) (noting that global e-commerce will represent a "trillion-dollar opportunity" by 2016). By 2016, Forrester predicts that "more than half of the dollars spent in U.S. retail will be influenced by the Web." SUCHARITA MULPURU ET AL., FORRESTER, US CROSS-CHANNEL RETAIL FORECAST, 2011 TO 2016 (2012).

5. *See, e.g.*, *The Local Network: Experian Analysis Highlights Which Countries Spend Longest on Facebook*, EXPERIAN (Sept. 27, 2011), http://www.experianplc.com /news/company-news/2011/27-09-2011.aspx ("Social networking is now one of the biggest online pastimes across the globe.").

6. Claire Cain Miller, *How Obama's Campaign Changed Politics*, N. Y. TIMES BITS BLOG (Nov. 7, 2008, 7:49 PM), http://bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics ("Mr. Obama used the Internet to organize his supporters in a way that would have in the past required an army of volunteers and paid organizers on the grounds . . . . Were it not for the Internet, Barack Obama would not be president."); *see* Megan Garber, *The Campaign Tumblr Is Dead! (Long Live the Campaign Tumblr!)*, THE ATLANTIC (Nov. 28, 2012, 5:33 PM), http://www.theatlantic.com/technology/archive/2012/11/the-campaign-tumblr-is-dead-long-live-the-campaign-tumblr/265688/ (discussing the first presidential campaign Tumblr).

7. WHITE HOUSE, CYBERSPACE POLICY REVIEW, *supra* note 2, at iii.

8. Jessica Bosari, *The Developing Role of Social Media in the Modern Business World*, FORBES (Aug. 8, 2012, 12:26 PM), http://www.forbes.com/sites /moneywisewomen/2012/08/08/the-developing-role-of-social-media-in-the-modern-business-world/ (asserting that social media marketing has become a "must" and citing a recent survey finding that "94% of all businesses with a marketing department used social media as part of their marketing platform").

9. Victoria Taylor, *Supply Chain Management: The Next Big Thing*, BLOOMBERG BUSINESSWEEK (Sept. 12, 2011), http://www.businessweek.com/business-schools/supply-chain-management-the-next-big-thing-09122011.html.

10. David Feinleib, *The 3 I's of Big Data*, FORBES (July 9, 2012, 4:05 PM), http://www.forbes.com/sites/davefeinleib/2012/07/09/the-3-is-of-big-data/ ("Big Data is . . . a transformative set of technological advances that have made analyzing data vastly more efficient."); Charles Duhigg, *How Companies Learn Your Secrets*, N.Y.

adoption of electronic payment solutions.[11] Moreover, the deployment of telecommunications technologies (e.g., videoconferencing) and collaborative software has reduced unnecessary business travel and improved collaboration across borders and time zones.

Second, IT has transformed societies. We work, shop,[12] and socialize[13] online. We embrace information technology's promise of improved healthcare (e.g., through personalized medicine,[14] telemedicine,[15] health-related mobile applications,[16] and big data analytics[17]), greater

---

TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all (describing major retailers' use of big data analytics to more efficiently market to consumers).

11. *See* Greg McAllister, *Mobile Payments: The Case for Choosing an Open Platform*, FORBES (Nov. 24, 2012, 8:44 PM), http://www.forbes.com/sites/ciocentral/2012/11/24/mobile-payments-the-case-for-choosing-an-open-platform/ (referencing efficiencies through mobile payments); MASTERCARD WORLDWIDE, BENEFITS OF OPEN PAYMENT SYSTEMS AND THE ROLE OF INTERCHANGE 8 (2008), http://www.mastercard.com/us/company/en/docs/BENEFITS%20OF%20ELECTRONIC%20PAYMENTS%20-%20US%20EDITION.pdf ("[Merchants using electronic payments] benefit by reducing costs associated with handling other forms of payment, including bounced checks, check verification and guarantee services, and check processing [as well as] collecting, counting, and transporting [cash].").

12. *See* Alistairr Barr, *Cyber Monday sales best ever, for Amazon's Kindle too*, CHI. TRIB. (Nov. 27, 2012), http://www.chicagotribune.com/business/sns-rt-us-amazon-kindlebre8aq0qt-20121127,0,4261081.story ("Internet sales jumped 30.3% on Cyber Monday [November 26, 2012] making it the biggest online shopping day ever. . . .").

13. JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RESEARCH CTR., THE FUTURE OF ONLINE SOCIALIZING 1 (2010), http://pewresearch.org/pubs/1652/social-relations-online-experts-predict-future ("[E]mail, social networks, and other online tools offer 'low friction' opportunities to create, enhance, and rediscover social ties that make a difference in people's lives. The internet lowers traditional communications constraints of cost, geography, and time; and it supports the type of open information sharing that brings people together.").

14. *See generally* DARRELL M. WEST, CTR. FOR TECH. INNOVATION AT BROOKINGS, ENABLING PERSONALIZED MEDICINE THROUGH HEALTH INFORMATION TECHNOLOGY: ADVANCING THE INTEGRATION OF INFORMATION 1 (2011), http://www.brookings.edu/~/media/research/files/papers/2011/1/28%20personalized%20medicine%20west/0128_personalized_medicine_west.pdf (discussing the challenges and concerns of implementing personalized healthcare through technology and offering possible solutions).

15. *See* Pam Belluck, *With Telemedicine as Bridge, No Hospital Is an Island*, N.Y. TIMES (Oct. 8, 2012), http://www.nytimes.com/2012/10/09/health/nantucket-hospital-uses-telemedicine-as-bridge-to-mainland.html?pagewanted=all&r=0.

16. *See* Joshua Brustein, *Coming Next: Using an App as Prescribed*, N.Y. TIMES (Aug. 19, 2012), http://www.nytimes.com/2012/08/20/technology/coming-next-doctors-prescribing-apps-to-patients.html.

17. Derrick Harris, *Better Medicine, Brought to You By Big Data*, GIGAOM (July 15, 2012, 6:00 AM), http://gigaom.com/cloud/better-medicine-brought-to-you-by-big-data/ (discussing the potential impact of big data analytics on genomics and current health-related applications for big data analytics including an effort to treat pediatric

democratization,[18] and improved quality of life for ourselves as individuals and as societies.[19]

Third, at the nation-state level, governments increasingly rely on IT solutions to provide cheaper, more efficient delivery of government services through e-government initiatives;[20] to manage their own supply chains;[21] to facilitate online voting;[22] and to carry out essential government functions, such as national defense.[23]

---

cancer based on the individual genetic profile of each affected child).

18. *See* RICHARD HUNDLEY ET AL., THE GLOBAL COURSE OF THE INFORMATION REVOLUTION: RECURRING THEMES AND REGIONAL VARIATIONS, RAND CORP. xxvii (2003), http://www.rand.org/content/dam/rand/pubs/monographreports/MR1680/MR1680.sum.pdf ("New political actors are being empowered by the information revolution—in the business, social, and political realms, at the subnational, transnational, and supranational levels—which is changing the distribution of political power.").

19. Press Release, United Nations, Information technology must be used to improve life in poor countries - Annan (Sept. 12, 2003), *available at* http://www.un.org/apps/news/story.asp?NewsID=8227&Cr=information&Cr1=technology (describing a video message from then-U.N. Secretary General Kofi Annan imploring UN Information and Communications Technology Task Force members to "spread the word" at the 2003 World Summit on the Information Society "about initiatives that make creative use of technology to improve the quality of life in developing countries").

20. *See* OFFICE OF E-GOV'T & INFO. TECH., OFFICE OF MGMT. & BUDGET, DIGITAL GOVERNMENT: BUILDING A 21ST CENTURY PLATFORM TO BETTER SERVE THE AMERICAN PEOPLE 27 (2012), http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf (describing the Obama Administration's strategy for "harnessing the power of technology to help create a 21st century digital government—one that is efficient, effective and focused on improving the delivery of services to the American people").

21. *See* HUNDLEY ET AL., *supra* note 18, at xxvii.

22. Although not generally accepted in the United States, other countries, such as the United Kingdom, Estonia, Switzerland, and Canada, have all begun to use Internet voting. Joanna Stern, *Why You Cannot Vote Online Today*, ABC NEWS (Nov. 6, 2012), http://abcnews.go.com/Politics/OTUS/election-day-vote-online-internet-today/story?id=17647954#.ULTveo4QgqY.

23. CHARLES BILLO & WELTON CHANG, INST. FOR SEC. TECH. STUDIES AT DARMOUTH COLL., CYBER WARFARE: AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES 3 (2004), http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf ("Information processing is becoming a 'center of gravity' in future warfare."); U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT 1 (2011), http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf ("Cyberspace is a critical enabler to Department of Defense (DoD) military, intelligence, business and, potentially, civil support operations."); BRYAN KREKEL ET AL., NORTHROP GRUMMAN CORP., OCCUPYING THE INFORMATION HIGH GROUND: CHINESE CAPABILITIES FOR COMPUTER NETWORK OPERATIONS AND CYBER ESPIONAGE 10 (2012), http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (describing the United States military's reliance on IT for vital "C4ISR" (i.e., command, control, communications, computers, intelligence, surveillance, and reconnaissance functions)); *see* COL. JASON SPADE, U.S.

Finally, at the international level, the growing global reliance on cyberspace has implications for established governance models,[24] alliances,[25] international stability,[26] and warfare.[27]

As we work to realize the extraordinary promise of cyberspace, we face

---

ARMY WAR COLL., INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 25 (Jeffrey Caton ed., 2012), http://www.carlisle.army.mil/dime/documents/China's%20Cyber%20Power%20and%20America's%20National%20Security%20Web%20Version.pdf ("The U.S. military is particularly cyber dependent, relying on a global network of 15,000 local area networks and 7 million computers connected by over 100,000 telecommunication circuits, spread across bases worldwide.").

24. *See* HUNDLEY ET AL., *supra* note 18, at xxvi ("Some traditional mechanisms of governance (e.g., taxation, regulation and licensing) are becoming increasingly problematic as the information revolution allows action beyond the reach of national governments."); Violet Blue, *U.S. Now 'Totally Unified' in Opposition to U.N. Internet Governance*, ZDNET (Dec. 6. 2012, 12:52 AM), http://www.zdnet.com/u-s-now-totally-unified-in-opposition-of-u-n-internet-governance-7000008382/ (reporting that, as the U.N.'s International Telecommunications Union considered proposals from various countries dealing with Internet regulation during the WCIT-12 summit in Dubai, the House of Representatives unanimously passed (397-0) a resolution intended to send a signal that the White House and Congress opposed any role the U.N. might take in Internet governance or regulation).

25. *See* NATO, DEFENDING THE NETWORKS: NATO POLICY ON CYBER DEFENCE (2011), http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (providing a coordinated approach to cyberdefense across the NATO Alliance); Press Release, NATO, Lisbon Summit Declaration (Nov. 20, 2010), *available at* http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease ("Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance . . . ."); NATO, STRATEGIC CONCEPT FOR THE DEFENCE AND SECURITY OF THE MEMBERS OF THE NORTH ATLANTIC TREATY ORGANISATION, ACTIVE ENGAGEMENT, MODERN DEFENCE ¶ 19 (2010), http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf ("We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. Therefore, we will: . . . develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations . . . .").

26. FRANKLIN D. KRAMER, ATLANTIC COUNCIL, ACHIEVING INTERNATIONAL CYBER STABILITY 14 (2012), http://www.acus.org/files/publication_pdfs/403/kramer_cyber_final.pdf (noting the establishment of a "cyber hot line" between the United States and Russia, and arguing that better resilience, cooperation, and transparency are necessary to enhance international cyber stability).

27. *See generally The Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO COOPERATIVE CYBER DEF. CENTRE OF EXCELLENCE, https://www.ccdcoe.org/249.html (last visited Mar. 27, 2013) (announcing the publication of the "Tallinn Manual," the result of a "three-year effort to examine how extant international law norms" apply to cyberwarfare).

an extraordinary challenge. Our shared digital infrastructure is vulnerable[28] to a wide-range of cyberthreats that are understood to pose some of the most serious economic and national security challenges of the 21st century (see *infra* Section IV).

II. SELF-REGULATION AND THE CHALLENGE OF CRITICAL INFRASTRUCTURE

The United States has adopted a largely self-regulatory, market-based approach to cybersecurity, relying on the private sector to secure its own networks. In keeping with this approach, no federal agency is responsible for defending the civilian (i.e., ".com") domain, and the federal government has avoided generally-applicable federal mandates regarding private sector cybersecurity practices.[29] Private sector companies have long understood that perfect security is unattainable, and, even if that were not the case, would be cost-prohibitive.[30] Accordingly, they must decide for themselves the optimal level of cybersecurity investment on a company-by-company basis.

A key challenge to the prevailing self-regulatory approach to private sector cybersecurity is the special problem of "critical infrastructures."[31] As explained in the National Strategy to Secure Cyberspace, which the

28. WHITE HOUSE, CYBERSPACE POLICY REVIEW, *supra* note 2, at iii; *see* WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 4 (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE] (describing digital infrastructure vulnerability to "natural disasters, accidents, and sabotage").

29. Companies handling certain types of sensitive personal data may be subject to sector-specific information security rules and also should be aware that the FTC has, under certain circumstances, set and enforced corporate data security obligations through both litigation and consent orders under its statutory authority to regulate "unfair" and "deceptive" trade practices pursuant to Section 5 of the FTCA. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, No. 12-cv-01365-SPL (D. Ariz. filed June 26, 2012), discussed in greater detail *infra* Section V.E.

30. *See, e.g.*, U.S. CHAMBER OF COMMERCE, INTERNET SECURITY ESSENTIALS FOR BUSINESS 2.0, at 3 (2012), http://www.uschamber.com/issues/technology/internet-security-essentials-business ("Perfect online security is unattainable . . . ."); *Public Fears in Virtual Places: Inaugural Cyber Security Lecture Tackles Crime, Solutions*, CABLE (July 21, 2012, 3:14 PM), http://cable.poly.edu/issue/news/public-fears-virtual-places-inaugural-cyber-security-lecture-tackles-crime-solutions (according to Marcus Sachs, Vice President of government affairs and national security policy at Verizon Communications, "perfection is impossible" and failures in cybersecurity are "inevitable").

31. Critical infrastructures are the "systems and assets, whether physical or virtual, so vital to the United States that the [incapacitation] or destruction of such systems and assets would have a debilitating effect on security, national economic security, national public health or safety, or any combination of those matters." Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c(e) (Supp. V 2011).

Department of Homeland Security ("DHS") released in 2003 in response to the 9/11 terrorist attacks:

> Our nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.[32]

Critical infrastructure networks are overwhelmingly owned and operated by individual private-sector companies; nevertheless, securing these networks is essential to U.S. economic and national security, particularly in view of the emerging threats of nation-state sponsored cyberespionage and cyberwarfare (see *infra* Sections III.B and III.C).

III. THE CHANGING FACE OF CYBERSECURITY: TECHNOLOGY TRENDS

Our nation's cybersecurity challenge is exacerbated by recent technology trends, most notably the: (1) explosive growth in mobile technology; (2) migration to cloud computing; and (3) pervasiveness of social networks.

A. Mobile Technology

Mobile technology continues to penetrate the global market, with the number of mobile devices expected to exceed the number of people on Earth by the end of 2016.[33] At the beginning of 2012, there already were nearly six billion mobile-cellular subscriptions (eighty-six percent "global

32. *National Strategy to Secure Cyberspace*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/national-strategy-secure-cyberspace (last visited Mar. 27, 2013). A prescient report from 1991 similarly described the risks of relying on information technology in a way that continues to resonate today. *See* NAT'L RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 7 (1991) ("We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.").

33. CISCO, CISCO VISUAL NETWORKING INDEX: CISCO GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2011–2016 3 (2013), http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI-Forecast_QA.pdf.

penetration") and more than one billion mobile-broadband subscriptions worldwide,[34] with the latter figure expected to jump to nearly five billion in 2016.[35] Simultaneously, the global mobile application market is exploding. While it accounted for just $1.7 billion in revenue globally in 2010,[36] it is expected to exceed $30 billion in revenue by the end of 2012[37] and reach $38 billion by 2015.[38] Apple's App Store and Google's Play Store each now offers 700,000 mobile applications for their respective platforms, iOS and Android OS.[39]

"Bring your own device," or "BYOD," is another important trend that has come with the penetration of mobile-broadband. Just a few years ago, Research-in-Motion's ("RIM") Blackberry device was the dominant player in the U.S. smartphone market, but new offerings from Apple, Google, and Microsoft have changed that, with consumers increasingly opting to purchase non-Blackberry devices.[40] For security reasons, it was once

34. *Key Statistical Highlights: ITU Data Release June 2012*, ITU WORLD TELECOMMS. (June 2012), http://www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf. As mobile penetration increases, the mobile advertising market is expected to continue on its own upward trajectory. Google alone earned $2.5 billion in mobile advertising revenue in 2011, and the mobile advertising market as a whole is expected to grow to $4.4 billion in the United States in 2013, with Facebook and Twitter projected to earn $72.7 million and $129.7 million in mobile advertising revenue, respectively, in 2012. *See* Rachel King, *Google's $8 Billion Mobile Ad Run Rate: The Fine Print*, ZDNET (Oct. 18, 2012, 9:12 PM), http://www.zdnet.com/googles-8-billion-mobile-ad-run-rate-the-fine-print-7000006019/ (explaining that the comparison between Google's $2.5 billion mobile advertising run rate for 2011 at the end of the third quarter and its projected $8 billion run rate for 2012 is "a bit like comparing apples and oranges" because the 2011 rate included "gross revenue from mobile ads" while the 2012 rate also includes "gross revenue from the mobile sales of Google Play content" and from "consumer spending on the Play apps"); Cotton Delo, *Facebook Tests Mobile-Ad Network, Challenging Google and Apple*, ADVERTISING AGE (Sept. 18, 2012), http://adage.com/article/digital/facebook-tests-mobile-ad-network-challenging-google-apple/237279/.

35. Press Release, Ericsson, Ericsson Predicts Mobile Data Traffic to Increase 10-Fold by 2016 (Nov. 7, 2011), http://hugin.info/1061/R/1561267/483146.pdf (predicting that mobile broadband subscriptions will reach nearly five billion in 2016, representing sixty percent year-on-year growth).

36. Austin Carr, *Report: Apps to Explode to $38 Billion Market by 2015*, FAST COMPANY (Mar. 1, 2011, 8:22 AM), http://www.fastcompany.com/1732635/apps-explode-38-billion-market-2015.

37. *Cumulative Mobile App Revenues Set to Exceed $30 Billion by End—2012*, ABI RESEARCH (Nov. 23, 2012), http://www.abiresearch.com/press/cumulative-mobile-app-revenues-set-to-exceed-30-bi.

38. Aemon Malone, *Report: Apps to Become $38 Billion Industry by 2015*, DIGITAL TRENDS (Mar. 1, 2011), http://www.digitaltrends.com/mobile/report-apps-to-become-38-billion-industry-by-2015/.

39. Damien Scott, *Google Play Store Now Has as Many Apps as Apple App Store*, COMPLEX (Oct. 30, 2012, 1:57 PM), http://www.complex.com/tech/2012/10/google-play-store-now-has-as-many-apps-as-apple-app-store.

40. In 2010, Research-in-Motion, which created the Blackberry, had thirty-nine

typical for U.S. corporations to require their employees to access corporate networks using only corporate-issued devices (typically BlackBerry devices, which earned top marks for enterprise security and was number one in the U.S. smartphone market).[41] Today's corporations increasingly permit employees to use mobile devices of their own choosing, including those offered by Apple (e.g., iPhone, iPad), Google (e.g., Android devices), and Microsoft.[42] Demand for the convenience and productivity offered by these devices may have started in corporate boardrooms, but it quickly trickled down to the rest of the corporate workforce and has put substantial pressure on corporations to loosen their previously restrictive corporate policies.

Mobile technology, by itself, poses a tremendous cybersecurity challenge. Smartphones equipped with internal microphones, cameras, and geolocation may be "the ultimate spy tool,"[43] enabling hackers to listen to calls made on the device, monitor text messages to and from the device, and track the location of the device.[44] Hackers could use a hacked phone

---

percent of the U.S. smartphone market. Today, it has just 9.5%. David Goldman, *BlackBerry's Wipeout Creates Major Mobile Security Gaps*, CNN MONEY (Sept. 26, 2012, 7:25 AM), http://money.cnn.com/2012/09/26/technology/mobile-security-byod/index.html.

41. *Id.*

42. Debra Cassens Weiss, *Bye-Bye BlackBerrys: 88% of BigLaw CIOs Expect Use to Decline in Next Year*, A.B.A. J. (Nov. 7, 2012, 5:30 AM), http://www.abajournal.com/news/article/bye-bye_blackberrys_88_of_large_firm_cios_expect_use_to_decline_in_next_yea (reporting that an *American Lawyer* survey of eighty-three Chief Information Officers ("CIOs") and technology chiefs at the nation's top law firms found that "eighty-eight percent of the CIOs expect a net drop in the number of BlackBerry users at their law firms in the next twelve months"). Apple's iPhone is reported to have roughly matched RIM's BlackBerry devices when it comes to enterprise security. Nick Heath, *iPhone Now as Secure as BlackBerry, Say Tech Chiefs*, TECHREPUBLIC (Sept. 18, 2012, 3:39 AM), http://www.techrepublic.com/blog/cio-insights/iphone-now-as-secure-as-blackberry-say-tech-chiefs/39749386.

43. Darlene Storm, *Mobile RAT Attack Makes Android the Ultimate Spy Tool*, COMPUTERWORLD (Mar. 1, 2012, 11:50 AM), http://blogs.computerworld.com/19803/mobile_rat_attack_makes_android_the_ultimate_spy_tool (quoting George Kurtz, former Chief Technology Officer of McAfee Labs); *see Smartphone Users Should Be Aware of Malware Targeting Mobile Devices and Safety Measures to Help Avoid Compromise*, FBI (Oct. 12, 2012), http://www.fbi.gov/scams-safety/e-scams (warning smartphone users regarding vulnerabilities in Android devices and suggesting preventative measures).

44. *See* Ken Dilanian, *New Security Flaw Discovered in Smartphones*, L.A. TIMES (Feb. 24, 2012), http://articles.latimes.com/2012/feb/24/business/la-fi-smartphone-hacking-20120224 ("[A cybersecurity researcher successfully] used a previously unknown hole in smartphone browsers to plant China-based malware that can commandeer the device, record its calls, pinpoint its location and access user texts and emails."). At the annual RSA Conference, security researchers recently offered a live demonstration of their successful "remote-access-tool" attack on an Android phone that

"as a hidden camera, secretly record video, tap into the microphone to eavesdrop or make audio recordings, and track your movements via GPS location."[45] Moreover, physical control over mobile devices is easily compromised due to their small size and portability,[46] and built-in security mechanisms are often unused[47] or easily circumvented, facilitating unauthorized third-party control over mobile devices.[48] Moreover, as devices become more functional, they often become less secure simply because there are more ways to introduce vulnerabilities: "Every app you install on your mobile device could lead to compromise, every text message you receive. Every website you browse using your own device's mobile browser is possibly suspect."[49]

In the BYOD environment, securing mobile devices is even more important. An employee's compromised device could be used to "listen in to business meetings for espionage or for insider trading"[50] or could serve as a "back door" into corporate networks.[51] Moreover, "[i]f just one device has been compromised—if a single employee clicks on a bad link, downloads a malicious app, or leaves the device at a bar—attackers could get a free pass into the network."[52] Corporations embracing the BYOD phenomenon may be "offering up a way into their networks on a silver platter."[53]

---

enabled them to activate the smartphone's microphone to listen to calls made on the device, monitor text messages to and from the targeted smartphone, and track the location of the device. CrowdStrike, *RSA 2012-Hacking Exposed: Mobile RATs (CrowdStrike)*, YOUTUBE (Mar. 4, 2012), http://www.youtube.com/watch?v=9smxU4gu8ac.

45. Storm, *supra* note 43.

46. WAYNE JANSEN & TIMOTHY GRANCE, NAT'L INST. OF SCIENCE AND TECH., GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING, SPECIAL PUBLICATION 800-144 viii (2011), http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

47. *Id.*; *see* Goldman, *supra* note 40 (reporting results of a Ponemon Institute study finding that fifty-nine percent of corporations that allow BYOD report that their employees fail to lock their personal devices, and fifty-one percent experienced some form of data loss as a result).

48. JANSEN & GRANCE, *supra* note 46, at viii.

49. Goldman, *supra* note 40.

50. Storm, *supra* note 43.

51. *See* Patrick Lambert, *BYOD: Risks, Rewards, and How to Deal with It*, TECHREPUBLIC (Nov. 1, 2012, 9:00 AM), http://www.techrepublic.com/blog/security/byod-risks-rewards-and-how-to-deal-with-it/8622 (noting the risk that an employee could bring an infected laptop that could open a back door into a network).

52. Goldman, *supra* note 40.

53. *Id.*

B. Cloud Computing[54]

Another important technology trend is the migration to cloud computing. Cloud computing is constantly evolving,[55] leading to some confusion over the precise contours of the term,[56] but "at the most basic level, cloud computing means that your data is stored on somebody else's computer."[57] It is generally agreed that cloud computing refers to delivering computing resources as a service over a network.[58] Cloud computing has been

54. The National Institute of Standards and Technology ("NIST") defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction," but cautions that "[c]loud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation." PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF SCIENCE AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING, SPECIAL PUBLICATION 800-145 1–2 (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. The NIST definition was the result of four years of work and fifteen draft definitions. *Final Version of NIST Cloud Computing Definition Published*, NIST (Oct. 25, 2011), http://www.nist.gov/itl/csd/cloud-102511.cfm. There are a number of competing theories regarding the origin of the term "cloud computing." Some assert that the term comes from "the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams." *See, e.g.*, Lakhmi Chand Goyal & Pradeep Kumar Jatav, *Cloud Computing: An Overview and Its Impact on Libraries*, 1 INT'L J. OF NEXT GENERATION COMPUTER APPLICATIONS 9, 9 (2012), http://ijngca.com/Papers/IJNGCA08092012.pdf. Others disagree. *See, e.g.*, John Willis, *Who Coined the Phrase Cloud Computing?*, IT MGMT. & CLOUD BLOG (Dec. 31, 2008), http://www.johnmwillis.com/cloud-computing/who-coined-the-phrase-cloud-computing/ (listing three different possibilities for the origins of the phrase).

55. Arif Mohamed, *A History of Cloud Computing*, COMPUTERWEEKLY (Mar. 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing ("Cloud computing has evolved through a number of phases which include grid and utility computing, application service provision (ASP), and Software as a Service (SaaS)."); *What Is The Cloud?*, GEN. SERVS. ADMIN., http://www.info.apps.gov/content/what-cloud (last visited Mar. 27, 2013) (discussing the evolution of today's cloud computing from grid and utility computing).

56. *Most Americans Confused by Cloud Computing According to National Survey*, CITRIX (Aug. 28, 2012), http://www.citrix.com/lang/English/lp/lp2328330.asp (reporting that most respondents in a recent survey believed the cloud is related to weather and that ninety-five percent of respondents who thought they were not using the cloud actually were).

57. *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 13 (2010) [hereinafter *ECPA Reform Hearing*] (statement of Edward W. Felten, Professor, Princeton University), http://judiciary.house.gov/hearings/printers/111th/111-149_58409.pdf.

58. *See, e.g., Computing: Services Overview*, ACCENTURE,

analogized to the modern high-rise office building: "[j]ust as a high-rise allows tenants to lease secure, individual offices in the same building while sharing core services such as plumbing and electricity, multi-tenant enterprise cloud computing allows organizations to use individualized software applications while sharing core computing services such as database and security."[59]

The reported benefits of cloud computing include scalability,[60] rapid deployment,[61] greater reliability,[62] efficiency,[63] increased storage,[64] flexibility,[65] business agility,[66] cost savings,[67] and energy savings.[68]

---

http://www.accenture.com/sk-sk/Pages/service-technology-cloud-computing-overview-summary.aspx (last visited Mar. 27, 2013) (defining cloud computing as "the dynamic provisioning of IT capabilities (hardware, software, or services) from third parties over a network"); *see also* Mohamed, *supra* note 55 ("The idea of an 'intergalactic computer network' was introduced in the sixties by J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network) [the predecessor to today's Internet] in 1969.").

59. *ECPA Reform Hearing*, *supra* note 57, at 44 (statement of David Schellhase, Executive Vice President & General Counsel, Salesforce.com).

60. *See ECPA Reform Hearing*, *supra* note 57, at 14 (statement of Edward W. Felten, Professor, Princeton University) ("[I]f [a] start-up's business grows rapidly and it needs to expand its computing capacity dramatically to handle a flood of new customers, this is easily done in the cloud, by simply increasing the number of servers the start-up is renting from the provider."); Andrew Nusca, *The Future of Cloud Computing: 9 Trends for 2012*, ZDNET (June 21, 2012, 3:26 AM), http://www.zdnet.com/blog/btl/the-future-of-cloud-computing-9-trends-for-2012/80511 (reporting that "scalability is driving adoption," with fifty-seven percent of companies in a recent poll identifying scalability as the most important reason they switched to the cloud).

61. MELL & GRANCE, *supra* note 54, at 2.

62. *See ECPA Reform Hearing*, *supra* note 57, at 14 (statement of Edward W. Felten, Professor, Princeton University).

63. *Id.* at 44 (statement of David Schellhase, Executive Vice President & General Counsel, Salesforce.com) ("By eliminating the need for costly and wastefully duplicative infrastructure, multi-tenant cloud computing frees users to focus on their core business, not their IT.").

64. Mohamed, *supra* note 55 (" 'Many IT professionals recognise the benefits cloud computing offers in terms of increased storage, flexibility and cost reduction,' said Songian Zhou, chief executive officer of *Platform Computing*.").

65. Rajani Baburajan, *The Rising Cloud Storage Market Opportunity Strengthens Vendors*, TMCNET (Aug. 24, 2011), http://technews.tmcnet.com/channels/cloud-storage/articles/211183-rising-cloud-storage-market-opportunity-strengthens-vendors.htm ("Cloud computing is becoming the preferred choice of organizations not only because of its cost savings but also because of the flexibility.").

66. *See id.* (observing that cloud computing enables enterprises to add capacity on demand).

67. *See id.*

68. Katie Fehrenbacher, *Cloud Computing Could Lead to Billions in Energy Savings*, GIGAOM (July 21, 2011, 8:48 AM), http://gigaom.com/2011/07/21/cloud-computing-could-lead-to-billions-in-energy-savings/ (reporting that cloud computing

By any measure, the market for cloud computing services is exploding. Global cloud computing revenue is projected to grow at a compound annual growth rate of 28.8% between now and 2015, and the market is expected to increase from $46 billion in 2009 to over $210 billion by 2015, according to analysts.[69]

Despite this rapid growth, many corporations are reluctant to embrace cloud-based solutions due to security concerns.[70] In a recent poll, more than half of the companies surveyed identified security as the reason that they have not adopted cloud computing technology.[71]

From a corporate cybersecurity perspective, the public cloud is a double-edged sword. It offers a number of potential benefits, including professionally managed security,[72] backup and recovery capabilities,[73] and

---

could lead to an estimated $12.3 billion in energy savings and 85.7 million metric tons of carbon emissions savings per year by 2020, according to AT&T-sponsored research); *id.* ("[M]oving business applications to the cloud could cut the associated per-user carbon footprint by 30 percent for large, already-efficient companies and as much as 90 percent for the smallest and least efficient businesses."); *see* Press Release, Pike Research, Cloud Computing to Reduce Global Data Center Energy Expenditures by 38% in 2020 (Dec. 6, 2010), *available at* http://www.pikeresearch.com/newsroom/cloud-computing-to-reduce-global-data-center-energy-expenditures-by-38-in-2020 (forecasting that cloud computing could lead to a thirty-eight percent reduction in worldwide data center energy use by 2020 due to substantial energy efficiency benefits); *Cloud Computing Energy Efficiency: Strategic and Tactical Assessment of Energy Savings and Carbon Emissions Reduction Opportunities for Data Centers Utilizing SaaS, IaaS, and PaaS,* NAVIGANT RES., http://www.pikeresearch.com/research/cloud-computing-energy-efficiency (last visited Mar. 27, 2013) ("[W]e anticipate that much of the work done today in internal data centers will be outsourced to the cloud by 2020, resulting in significant reductions in energy consumption, associated energy expenses, and GHG emissions from data center operations versus a business as usual (BAU) scenario.").

69. *Cloud Computing Energy Efficiency*, *supra* note 68; Press Release, Gartner, Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010 (June 22, 2010), *available at* http://www.gartner.com/it/page.jsp?id=1389313 (reporting that the worldwide market for cloud services will be worth $148.8 billion by 2014); *accord*, Louis Columbus, *Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth*, FORBES, (Feb. 19, 2013, 12:36 PM), http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/ (reporting that global spending on public cloud services is expected to achieve a compound annual growth rate of 17.7% from 2011 through 2016 and that the worldwide market for cloud services is expected to grown from $76.9 billion in 2010 to $210 billion in 2016).

70. Robert Scheier, *Cloud Computing Tools: Improving Security Through Visibility and Automation*, CSO ONLINE (May 14, 2012), http://www.csoonline.com/article/706357/cloud-computing-tools-improving-security-through-visibility-and-automation.

71. Nusca, *supra* note 60 (reporting the results of a North Bridge Venture Partners poll of 785 people at thirty-nine enterprise technology companies, which noted a concern regarding regulatory compliance and vendor lock-in as additional reasons for inhibition of adoption of cloud-computing).

72. *ECPA Reform Hearing*, *supra* note 57, at 13 (statement of Edward W. Felten, Professor, Princeton Univ.). Cloud provider reliance on "dedicated personnel" to

automation of vulnerability mitigation and security management functions[74] (although automation may be prohibitively expensive for many companies[75]). But other characteristics of cloud computing—including system complexity,[76] the multi-tenant environment,[77] and loss of control[78]—pose significant challenges to corporate cybersecurity.[79]

---

maintain security, manage software updates, and "continually strengthen" security measures could boost corporate security. *Advancements in Cloud Security*, DLT SOLUTIONS, http://www.dlt.com/technology/cloud-computing/understanding-cloud-computing/cloud-security/advancements-in-cloud-securi (last visited Mar. 27, 2013). Indeed, "[c]loud providers . . . have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization. Increases in the scale of computing induce specialization, which in turn allows security staff to shed other duties and concentrate exclusively on security issues. Through increased specialization, there is an opportunity for staff members to gain in-depth experience, take remedial actions, and make security improvements more readily than otherwise would be possible with a diverse set of duties." JANSEN & GRANCE, *supra* note 46, at 9.

73. JANSEN & GRANCE, *supra* note 46, at 9–10. ("Redundancy and disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when faced with increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents.").

74. 3rdID8487, *Cyber Security and American Power*, YOUTUBE, at 34:30 (July 11, 2012), http://www.youtube.com/watch?v=nTwiZneMw3U [hereinafter *Keith Alexander's Remarks*]. JANSEN & GRANCE, *supra* note 46, at 9 ("Greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities [such as] configuration control, vulnerability testing, security audits, and security patching of platform components. Information assurance and security response activities also profit from a uniform, homogeneous cloud infrastructure . . . ."); Scheier, *supra* note 70 ("[T]he same automated, consistent provisioning that is essential to managing either public or private clouds . . . can also offer the fringe benefit of improving security . . . . Because so many security vulnerabilities are caused by human error, automating proper server configuration also automatically improves security . . . . Automated server provisioning tools . . . help prevent variations that could create vulnerabilities . . . . [and] enable administrators to easily control common security-sensitive settings, such as which ports are open and which services are running.").

75. Scheier, *supra* note 70 ("[H]igh [per server] costs force organizations with thousands of servers to go without automated patch or configuration management or audit compliance . . . relying instead on scripts or manual processes.").

76. JANSEN & GRANCE, *supra* note 46, at 10–11 ("Many components make up a public cloud, resulting in a large attack surface . . . . Security depends not only on the correctness and effectiveness of many components, but also on the interactions among them.").

77. *Id.* at 11 ("Having to share an infrastructure with unknown outside parties can be a major drawback for some applications . . . .").

78. *Id.* at 12 ("Loss of control over both the physical and logical aspects of the system and data diminishes the organization's ability to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security . . . that are in the best interest of the organization.").

79. *See generally id.*; *see also* Jon Brodkin, *Gartner: Seven Cloud-Computing*

Moreover, many cloud characteristics themselves are double-edged swords. Take data concentration, for example. Concentrating data in the cloud may expose data to fewer risks than a more distributed model in which data resides on mobile devices, laptops, or other peripherals that can be lost or stolen. However, consolidating data in one location creates an attractive target and could render a successful security breach disastrous.[80] Likewise, a uniform cloud infrastructure may benefit information assurance activities, but may enable "a single flaw [to] manifest[] throughout the cloud, potentially impacting all tenants and services."[81]

C. Social Networking

The rise of social networking also brings new cybersecurity challenges. Hackers have long relied on "social engineering"—convincing people to disclose information that they should not[82]—to gain the trust of targets and compromise their networks. Now, detailed information gleaned from social networking sites is helping adversaries successfully target even the most sophisticated corporate victims through social engineering.[83]

The May 2011 attack on RSA Security ("RSA"), one of the nation's oldest and best-known security technology companies, serves as a cautionary tale regarding how adversaries use social engineering to compromise their victims' networks. In RSA's case, a spear-phishing email (i.e., an email used to "target specific people at enterprises with the aim of gaining a foothold into the corporate network"[84]) was sent to two

---

Security Risks, INFOWORLD (July 2, 2008), http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

80. Mathew J. Schwartz, *Epsilon Fell to Spear-Phishing Attack*, INFORMATIONWEEK (Apr. 11, 2011, 3:55 PM), http://www.informationweek.com/security/attacks/epsilon-fell-to-spear-phishing-attack/229401372 ("The Epsilon breach highlights that with the growth of cloud services, one data breach can be a single point of failure for numerous organizations . . . . [E]ntrusting a single company with data on so many people makes it an attractive target for attackers, which may in fact place customers at greater risk of having their personal information stolen.").

81. JANSEN & GRANCE, *supra* note 46, at 9.

82. Matthew Weinschenk, *CyberSecurity's Biggest Threat is Decidedly Low Tech*, WALL ST. DAILY (Mar. 8, 2012), http://www.wallstreetdaily.com/2012/03/08/cyber-securitys-biggest-threat/.

83. JANSEN & GRANCE, *supra* note 46, at viii ("The growing availability and use of social media, personal Webmail, and other publicly available sites are a concern, since they increasingly serve as avenues for social engineering attacks that can negatively impact the security of the client, its underlying platform, and cloud services accessed.").

84. Robert Westervelt, *Study Finds Spear Phishing at Heart of Most Targeted Attacks*, SEARCHSECURITY (Nov. 29, 2012), http://searchsecurity.techtarget.com/news/2240173534/Study-finds-spear-phishing-at-heart-of-most-targeted-attacks; TRENDMICRO INC., SPEAR-PHISHING EMAIL: MOST FAVORED ATTACK BAIT 1–2 (2012), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-

groups of RSA employees. The subject of the email message was "2011 Recruitment Plan." Attached to the email was a malware-embedded[85] Excel spreadsheet innocuously entitled "2011 Recruitment plan.xls."[86] Although RSA's systems automatically identified and marked the email as "junk," one employee opened the email, thereby unwittingly releasing the malware that ultimately facilitated the exfiltration of sensitive data.[87]

Spear-phishing also was the *modus operandi* in the 2011 attack on Epsilon, an email marketing behemoth. In that attack, an estimated sixty million email addresses were compromised, resulting in an estimated $225 million in costs to Epsilon from the data breach alone.[88] Phishers could

---

papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf ("In a typical spear-phishing attack, a specially crafted email is sent to specific individuals from a target organization. The recipients are convinced through clever and relevant social engineering tactics to either download a malicious file attachment or to click a link to a malware- or an exploit-laden site . . . . [This] installs a malware in a compromised computer. The malware then accesses a malicious command-and-control (C&C) server to await instructions from a remote user. At the same time, [the malware] usually drops a decoy document that will open when the malware or exploit runs to hide malicious activity."). *Id.* at 1 ("[S]pear phishing makes use of information about a target to make attacks more specific and 'personal' to the target. Spear-phishing emails, for instance, may refer to their targets by their specific name, rank, or position instead of using generic titles as in broader phishing campaigns."). A paradigmatic example of spear-phishing came to light as a result of the long-running cyberbattle between the nation-states of Georgia and Russia. In this intriguing case, a Russian hacker believed to be seeking sensitive Georgian government documents on behalf of Russian intelligence "sent a series of emails to [Georgian] government officials that appeared to come from the president of Georgia, with the address 'admin@president.gov.ge.' Those emails contained a malicious PDF attachment, purportedly containing legal information, with an exploit that delivered malware." Jeremy Kirk, *Georgia Outs Russia-Based Hacker—With Photos*, PC WORLD (Oct. 30, 2012, 11:20 AM), http://www.pcworld.com/article/2013289/georgia-outs-russia-based-hacker-with-photos.html.

85. *Malware (Malicious Software)*, SEARCHMIDMARKETSECURITY, http://searchmidmarketsecurity.techtarget.com/definition/malware (last updated Oct. 2008) ("Malware . . . is any program or file that is harmful to a computer user.").

86. Peter Bright, *Spearphishing + Zero-Day: RSA Hack* Not *"Extremely Sophisticated,"* ARS TECHNICA, (Apr. 4, 2011, 4:17 PM), http://arstechnica.com/security/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated/.

87. Opening the email attachment led to installation of a variant of the Poison Ivy RAT. A RAT is "a Remote Administration/Access Tool/Toolkit/Trojan. RATs allow remote access to files, the registry, monitoring of network access, starting and stopping programs, and more, making them extremely powerful: anything the user can do locally, the hacker can do remotely . . . . With Poison Ivy installed, the attacker stole user credentials and escalated their privileges to gain access to secure systems that the originally compromised user didn't have access to. The attacker then used this system access to exfiltrate . . . sensitive data . . . ." *Id.*

88. *Total Cost of Epsilon E-mail Breach Could Reach $225M, Including up to $45M in Lost Business, According to New Report by CyberFactors*, BUS. WIRE (Apr. 29, 2011, 12:29 PM), http://www.businesswire.com/news/home/20110429005630/en/Total-Cost-Epsilon-E-Mail-Data-Breach-Reach.

further exploit the compromised email addresses, leading some to project that the Epsilon breach could generate up to $4 billion in total costs, including fines, litigation, lost business, forensic audits, and monitoring.[89]

As corporate security improves, adversaries increasingly rely on "social engineering" to gain the trust of targets, to convince people to disclose information that they should not,[90] and subsequently to compromise targets' networks. Thirty-seven percent of records compromised through cyber data breaches were compromised as a result of incidents employing social tactics.[91] Moreover, industry data suggest that spear-phishing is at the heart of most targeted attacks.[92]

Government and private sector cybersecurity experts warn that hackers increasingly are exploiting information gleaned from social networking sites for social engineering-based attacks. For example, the FBI warns that "[p]redators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation."[93] Security provider Trend Micro warns:

> While human-related information like a target's name, job title, and email address may be bought from the underground market or be provided by the masterminds behind sanctioned attacks, the Internet is the most convenient source of such information. Social networking sites, corporate and academic publications, and organizations' sites allow miscreants to harvest relevant information on their targets for various social engineering schemes.[94]

Indeed, "[e]lite cybercriminals are tapping into search engines and social networks to help them target specific employees for social-engineering trickery at a wide range of companies, professional firms and government agencies."[95]

---

89. *Id.*

90. Weinschenk, *supra* note 82.

91. VERIZON, VERIZON'S 2012 DATA BREACH INVESTIGATIONS REPORT 33 (2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

92. Ninety-one percent of targeted attacks involved spear-phishing, and ninety-four percent of emails contained malicious file attachments, according to TrendMicro's analysis of targeted attack data collected between February and September of 2012. *See* TRENDMICRO INC., *supra* note 84, at 1.

93. FBI, U.S. DEP'T OF JUSTICE, INTERNET SOCIAL NETWORKING RISKS 2, http://www.ncix.gov/issues/cyber/internet-social-networking-risks.pdf.

94. TRENDMICRO INC., *supra* note 84, at 5.

95. Byron Acohido, *Social-Media Tools Used to Target Corporate Secrets*, USA TODAY (Mar. 31, 2011), http://usatoday30.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm ("[M]any attacks [that cybersecurity firm] Mandiant has investigated began with the criminals doing reconnaissance on Google, Facebook, LinkedIn, Twitter and other popular Internet services to find companies to

IV. THE CHANGING FACE OF CYBERSECURITY: CYBERTHREAT TRENDS

There are only two types of companies in this country: those who know they have been hacked, and those who don't.[96]

Cybercrime,[97] cyberespionage,[98] and cyberwarfare[99] have long been understood to threaten the security of cyberspace, however the gravity of the cyberthreat recently has been publicly underscored with increasing frequency at the highest levels of the United States government. President Obama penned a *Wall Street Journal* op-ed in August 2012 describing the cyberthreat as "one of the most serious economic and national security challenges" facing our nation.[100] Six months later, he emphasized the importance of cybersecurity in his post-election State of the Union address,

---

target—and pinpoint specific executives, researchers, analysts, engineers or key administrative assistants to attack. The next step is to craft a spear-phishing lure designed to entice a specific employee to click on a viral attachment or Web page link, using information gleaned during the reconnaissance phase to make the attachment or link seem trustworthy.").

96. Although the precise origin of this statement appears to be unknown, it is used quite frequently in cybersecurity circles. *See, e.g.*, DMITRI ALPEROVITCH, MCAFEE, REVEALED: OPERATION SHADY RAT 2 (2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf ("I divide the entire set of Fortune Global 2,000 firms into two categories: those that *know they've been compromised*, and those that *don't yet know*.") (emphasis in original); Jonathan Fisher, *China Has Hacked Every U.S. Major Company, Claims Richard Clarke*, WEBPRONEWS (Mar. 28, 2012), http://www.webpronews.com/china-has-hacked-every-u-s-major-company-claims-richard-clarke-2012-03 (" 'There are two kinds of companies: those that have been hacked, and those that will be.' If you listen to people talk about cyber security long enough, you'll hear a hundred subtle variations of that statement. Another version goes: 'There are two kinds of companies: those that know they've been hacked, and those that don't,' implying that every server and every computer the world over is not only vulnerable to attack, but has at least been probed in the past.").

97. *See, e.g.*, Meredith Johnston, *Cybercrime is on the rise*, TECHREPUBLIC (June 16, 2000, 7:00 AM), http://www.techrepublic.com/article/cybercrime-is-on-the-rise/5032146 (illustrating twelve types of cybercrime, including financial fraud, denial of service, and theft of proprietary information).

98. *See, e.g.*, Nathan Thornburg, *Inside the Chinese Hack Attack*, TIME (Aug. 25, 2005), http://www.time.com/time/nation/article/0,8599,1098371,00.html.

99. *See, e.g.*, John Stanton, *Rules of Cyber War Baffle U.S. Government Agencies*, NAT'L DEF. MAG. (Feb. 2000), http://www.nationaldefensemagazine.org/archive/2000/February/Pages/Rules4391.aspx; *U.S. Army Kick-Starts Cyber War Machine*, CNN (Nov. 22, 2000), http://articles.cnn.com/2000-11-22/tech/cyberwar.machine.idg_1_computer-viruses-denial-of-service-cyberwarfare?_s=PM:TECH.

100. Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012, 7:15 PM), http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

declaring: "America must . . . face the rapidly growing threat."[101] In March 2013, just one year after FBI Director Robert Mueller warned that cyberthreats were expected to surpass terrorism as the single "greatest threat" to the United States,[102] the U.S. Director of National Intelligence ("DNI") publicly identified cyber as the top global threat facing America, stating "it's hard to overemphasize its significance."[103] The next day, President Obama invited select CEOs of critical infrastructure companies directly to the White House to discuss cybersecurity,[104] and a few weeks later, in April 2013, he "summoned 15 of America's top financial leaders to the White House to discuss . . . cyberrisks."[105]

Throughout 2012, other top national security officials also publicly emphasized the gravity of the cyberthreat. In February 2012, former Director of the National Security Agency ("NSA") and former DNI, Mike McConnell, said: "The United States is fighting a cyberwar today, and we are losing."[106] In October 2012, then-Defense Secretary Leon Panetta warned that the United States is at risk for a "cyber Pearl Harbor,"[107] saying

---

101. Barack Obama, Remarks by the President in the State of the Union Address (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address. The President took the opportunity afforded by his State of the Union address to signal his intention to make cybersecurity a priority in his second term and to lay out his plan for doing so, stating: "Earlier today, I signed a new executive order that will strengthen our cyber defenses . . . . But now Congress must act as well, by passing legislation to give our government a greater capacity to secure our networks and deter attacks. This is something we should be able to get done on a bipartisan basis." *Id.*

102. Stacy Cowley, *FBI Director: Cyberthreat will eclipse terrorism*, CNN MONEY, (Mar. 2, 2012, 7:55 AM), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm (quoting FBI Director Mueller saying: "Terrorism does remain the FBI's top priority, but in the not too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country").

103. *Worldwide Threat Assessment: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 5–6 (2013) (remarks by James R. Clapper, Director of Nat'l Intelligence), http://www.dni.gov/files/documents/Intelligence%20Reports/WWTA%20Remarks%20as%20delivered%2012%20Mar%202013.pdf.

104. Alex Mooney, *President to Host CEOs in Situation Room for Cyber Security Chat*, CNN (Mar. 13, 2013, 1:22 PM), http://security.blogs.cnn.com/2013/03/13/president-to-host-ceos-in-situation-room-for-cyber-security-chat/.

105. Frederick Kempe, *Seeking to Avert Cyberwar*, April 15, 2013. http://blogs.reuters.com/thinking-global/2013/04/15/seeking-to-avert-cyber-war/. An executive who participated in the April meeting explained: "[t]he President scared the hell out of all of us, and we're not easy to frighten." *Id.*

106. Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST (Feb. 28, 2012), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493pf.html.

107. Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on US*, N.Y. TIMES (Oct. 11, 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

"[t]his is a pre—9/11 moment."[108] Finally, with respect to cyberespionage, Richard Clarke, former counterterrorism czar in the Clinton and both Bush administrations, warned of an impending "death of a thousand cuts [whereby] we lose our competitiveness by having all of our research and development stolen by the Chinese."[109]

Whatever one may think of the merits of these claims,[110] it is clear that despite corporate America's increasing awareness of, and investment in, cybersecurity, our digital assets and infrastructure routinely are being exploited. U.S. victims of major cyberincidents[111] over the past few years

---

108. Julian E. Barnes & Siobhan Gorman, *U.S. Readies Cyberdefense*, WALL ST. J. (Oct. 11, 2012, 10:29 PM), http://online.wsj.com/article /SB10000872396390444657804578051071681887566.html.

109. Emil Protalinski, *Richard Clarke: China Has Hacked Every Major US Company*, ZDNET (Mar. 27, 2012, 6:04 AM), http://www.zdnet.com/blog/security /richard-clarke-china-has-hacked-every-major-us-company/11125.

110. Bruce Schneier, *The Threat of Cyberwar Has Been Grossly Exaggerated*, SCHNEIER ON SECURITY (July 7, 2010, 12:58 PM), http://www.schneier.com/blog /archives/2010/07/the_threat_of_c.html ("[T]he entire national debate on cyberwar is plagued with exaggerations and hyperbole."); Maggie Shiels, *Cyber War Threat Exaggerated Claims Security Expert*, BBC (last updated Feb. 16, 2011, 4:21 AM), http://www.bbc.co.uk/news/technology-12473809 (reporting on claims that the threat of cyberwar is greatly exaggerated and quoting security expert Bruce Schneier, who said that, instead of cyberwar, "we are seeing . . . an increasing use of war-like tactics and that is what is confusing us"); Barnes & Gorman, *supra* note 108 (explaining that, according to one expert, then-Secretary Panetta's remarks "described the gravest attack Americans might face, not the most likely," and that the 9/11 tragedy in which over 3,000 people died is "an unlikely scenario for a cyberthreat . . . in the near term").

111. Although this Article focuses on the United States, other countries are not immune from cyberexploitation, as recent breaches involving foreign aerospace, defense, and manufacturing industries illustrate. *See, e.g.*, *Japan Confesses Data Breach on Epsilon Rocket*, VOICE OF RUSSIA (Dec. 3, 2012, 2:04 PM), http://english.ruvr.ru/2012_11_30/Japan-confesses-data-breach-on-Epsilon-rocket/ (describing a recent breach at the Japan Aerospace Exploration Agency ("JAXA") that resulted in exfiltration of sensitive data about Japan's rocket program, including the "parameters" and "specifics of engine maintenance" for Japan's solid-fueled Epsilon Rocket). Notably, solid-fuel rockets of Epsilon's size can be used as intercontinental ballistic missiles. *See also* Matteo Emanuello, *Epsilon Rocket Data Stolen by Hackers*, SPACE SAFETY MAGAZINE (Dec. 5, 2012, 4:36), http://www.spacesafetymagazine.com /2012/12/05/epsilon-rocket-data-stolen-hackers/; Nicole Perlroth, *Nissan Is Latest Company to Get Hacked*, N.Y. TIMES BITS BLOG (Apr. 24, 2012, 12:34 PM), http://bits.blogs.nytimes.com/2012/04/24/nissan-is-latest-company-to-get-hacked/ ("Nissan confirmed its computer systems were hacked . . . . The attack is just the latest in a string of cyberattacks on corporations . . . ."); Eric Savitz, *Military Contractor Mitsubishi Heavy Hit by Hack Attack*, FORBES (Sept. 19, 2011, 12:43 PM), http://www.forbes.com/sites/ericsavitz/2011/09/19/military-contractor-mitsubishi-heavy-hit-by-hack-attack/ (describing a "major hack attack" on Mitsubishi Heavy Industries in which data reportedly was exfiltrated from "the Japanese industrial giant that makes submarines, missiles and components for nuclear power plants"). David Leppard, *Chinese Steal Jet Secrets from BAE*, THE SUNDAY TIMES (Mar. 11, 2012), http://www.thesundaytimes.co.uk/sto/news/uk_news/National/article991581.ece ("Chinese spies hacked into computers belonging to BAE Systems, Britain's biggest

include: U.S. Chamber of Commerce (May 2010),[112] Google (June 2010),[113] RSA Security (May 2011),[114] Sony (May 2011; October 2012),[115] Booz Allen Hamilton (July 2011),[116] U.S.-China Economic and Security Review Commission (September 2011),[117] twenty-three natural gas pipeline operators (December 2011–June 2012),[118] Global Payments (March 2012),[119] numerous financial services companies and the New York Stock Exchange (September 2012–March 2013),[120] the White House

---

defence company, to steal details about the design, performance and electronic systems of the West's latest fighter jet . . . prompt[ing] fears that the jet's radar capabilities could have been compromised.").

112. Nicole Perlroth, *Hacked Chamber of Commerce Opposed Cybersecurity Law*, N.Y. TIMES BITS BLOG (Dec. 21, 2011, 6:10 PM), http://bits.blogs.nytimes.com /2011/12/21/hacked-chamber-of-commerce-opposed-cybersecurity-law/ ("The United States Chamber of Commerce has confirmed Chinese hackers last year broke into internal networks.").

113. *See infra* note 158.

114. Riva Richmond, *The RSA Hack: How They Did It*, N.Y. TIMES BITS BLOG (Apr. 2, 2011, 3:17 PM), http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/.

115. Christopher MacManus, *Sony's PlayStation 3 Experiences Its Biggest Hack Yet*, CNET (Oct. 24, 2012, 7:48 PM), http://news.cnet.com/8301-17938_105-57539756-1/sonys-playstation-3-experiences-its-biggest-hack-yet/; Jason Shreier, *Sony Hacked Again; 25 Million Entertainment Users' Info at Risk*, WIRED (May 2, 2011, 7:11 PM), http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack/.

116. Andy Greenberg, *Anonymous Hackers Breach Booz Allen Hamilton, Dump 90,000 Military E-Mail Addresses*, FORBES (July 11, 2011), http://www.forbes.com/sites/andygreenberg/2011/07/11/anonymous-hackers-breach-booz-allen-hamilton-dump-90000-military-email-addresses/.

117. Mark Hosenball, *U.S. Authorities Probe U.S.-China Commission Email Hack*, REUTERS (Jan. 10, 2012, 7:09 AM), http://www.reuters.com/article/2012/01/10/us-usa-india-hacking-idUSTRE80828N20120110 ("U.S. authorities are investigating allegations that an Indian government spy unit hacked into emails of [USCC,] an official U.S. commission that monitors economic and security relations between the United States and China, including cyber-security issues.").

118. Mark Clayton, *Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage*, CHRISTIAN SCI. MONITOR (Feb. 27, 2013), http://www.csmonitor.com /Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage.

119. The breach of credit card payment processor Global Payments, Inc. potentially exposed personal information, card numbers, and card-verification codes associated with millions of Visa and MasterCard cardholders. Global Payments estimates that the breach affected at least 1.5 million accounts in North America and cost the company $93.9 million dollars. Info. Sec. Media Grp., *Global Payments Breach Tab: $94 Million*, BANK INFO SEC. (Jan. 10, 2013), http://www.bankinfosecurity.com /global-payments-breach-tab-94-million-a-5415/op-1.

120. Tracy Kitten, *DDoS: 6 Banks Hit On Same Day*, BANK INFO SEC. (Mar. 14, 2013), http://www.bankinfosecurity.com/ddos-6-banks-hit-on-same-day-a-5607 ("Six leading U.S. banking institutions were hit by distributed-denial-of-service attacks on March 12, the largest number of institutions to be targeted in a single day."); Perlroth, *supra* note 112 (describing a massive distributed denial of service attack with

(September 2012),[121] Nationwide Mutual Insurance Company (October 2012),[122] major U.S. media outlets including the New York Times[123] and Wall Street Journal (October 2012–January 2013),[124] the Alabama State Government (January 2013),[125] the U.S. Sentencing Commission (January 2013),[126] the U.S. Probation Office for the Eastern District of Michigan,[127] Evernote (March 2013),[128] and Reddit (April 2013).[129] Large-scale cyberoperations uncovered during the same time period include Red October, an alleged Chinese cyberespionage operation uncovered in October 2012,[130] and a massive operation discovered in early 2013 that

---

"unprecedented" volume of traffic affecting U.S. financial institutions, including Wells Fargo, U.S. Bank, PNC, the New York Stock Exchange, and others).

121. Jana Winter & Jeremy A. Kaplan, *White House Confirms Chinese Hack Attack on White House Computer*, FOX NEWS (Oct. 1, 2012), http://www.foxnews.com/tech/2012/10/01/washington-confirms-chinese-hack-attack-on-white-house-computer/.

122. *Nationwide Insurance Says Data Breach Affects 1.1M*, ASSOCIATED PRESS – THE BIG STORY (Dec. 5, 2012, 4:03 PM), http://bigstory.ap.org/article/nationwide-insurance-says-data-breach-affects-11m.

123. Nicole Perlroth, *Hackers in China Attacked the Times for Last 4 Months*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

124. Siobhan Ghorman et al., *Chinese Hackers Hit U.S. Media*, WALL ST. J. (Jan. 31, 2013, 8:28 PM), http://online.wsj.com/article/ SB10001424127887323926104578276202952260718.html ("[The Wall Street Journal's] computer systems had been infiltrated by Chinese hackers, apparently to monitor its China coverage.").

125. Press Release, Office of the Ala. Dep't of Homeland Sec., ALDHS Director Details Cyber Intrusion in State IT System (Jan. 29, 2013), *available at* http://www.homelandsecurity.alabama.gov/news_detail.aspx?ID=7511.

126. Will Oremus, *Aaroz Swartz Protestors Take Over Government Websites, Install Asteroids*, SLATE (Jan. 28, 2013, 10:27 AM), http://www.slate.com /blogs/future_tense/2013/01/28/aaron_swartz_protest_anonymous_hacks_government_websites_installs_asteroids.html ("As part of its ongoing protest of the U.S. government's prosecution of computer programmer and activist Aaron Swartz, [hackers affiliated with the group known as] Anonymous . . . hacked the website of the U.S. Sentencing Commission . . . .").

127. *Id.*

128. Doug Gross, *50 Million Compromised in Evernote Hack*, CNNTECH (Mar. 4, 2013, 4:34 PM), http://www.cnn.com/2013/03/04/tech/web/evernote-hacked/ (publicizing hack of Evernote, an online note-taking and archiving service with 50 million users, in which hackers accessed a variety of user information, including user names, e-mail addresses, and encrypted passwords).

129. Dan Kaplan, *Reddit site downed by DDoS attacks*, SC MAGAZINE (Apr. 19, 2013), http://www.scmagazine.com/reddit-site-downed-by-ddos-attacks/article/289680/.

130. Mathew J. Schwartz, *Operation Red October Attackers Wielded Spear Phishing*, INFORMATIONWEEK (January 18, 2013, 3:06 PM), http://www.informationweek.com/security/attacks/operation-red-october-attackers-wielded/240146621 ("The primary focus of this campaign targets countries in Eastern Europe, former USSR republics, and countries in Central Asia, although victims can be found everywhere, including Western Europe and North America.").

victimized Apple,[131] Facebook,[132] Twitter,[133] Microsoft,[134] and an estimated forty other companies.[135]

A. Cybercrime

The term cybercrime is used to refer both to traditional crimes (e.g., extortion,[136] fraud, forgery, identity theft, and child exploitation) that are committed over electronic networks and information systems as well as to crimes unique to electronic networks (e.g., hacking and denial of service attacks).

1. Costs of Cybercrime

By all measures, cybercrime is flourishing.[137] Symantec's Norton estimates global cybercrime costs at $114 billion annually ($388 billion

131. Jim Finkle & Joseph Menn, *Exclusive: Apple, Macs Hit by Hackers Who Targeted Facebook*, REUTERS (Feb. 19, 2013, 4:50 PM), http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91110920130219 ("The breaches described by Apple mark the highest-profile cyber attacks to date on businesses running Mac computers."). The hackers are believed to have used a browser-based Java exploit.

132. Doug Gross, *Eastern European Gang Hacked Apple, Facebook, Twitter*, CNNTECH (Feb. 20, 2013, 12:19 PM), http://www.cnn.com/2013/02/20/tech/web/hacked-apple-facebook-twitter/index.html?iref=allsearch.

133. Mathew Schwartz, *Twitter Pursues Two Factor Authentication After Password Breach*, INFORMATIONWEEK (Feb. 4, 2013, 3:06 PM), http://www.informationweek.com/security/application-security/twitter-pursues-two-factor-authenticatio/240147787 ("[Twitter detected] a security breach affecting an estimated 250,000 of its 250 million users.").

134. *Microsoft Hacked: Intrusion Was 'Similar' to Apple and Facebook Hacks*, HUFFINGTON POST (Feb. 22, 2013), http://www.huffingtonpost.com/2013/02/22/microsoft-hacked-apple-hacked-facebook-hacked_n_2745178.html.

135. Dara Kerr, *Apple, Facebook Hackers Hit Car and Candy Companies, Too*, CNET (Mar. 11, 2013, 5:49 PM), http://news.cnet.com/8301-1009_3-57573720-83/apple-facebook-hackers-hit-car-and-candy-companies-too/?utm_medium=twitter ("At least some of these hacks are thought to have originated in Eastern Europe while others are suspected to have come from China. It is unclear if all of the companies were targeted by one group of hackers or if they were isolated incidents.").

136. *See, e.g.*, GAVIN O'GORMAN & GEOFF MCDONALD, SYMANTEC RANSOMWARE: A GROWING MENACE 1–2, http://www.symantec.com/content/en/us/enterprise/media/securityresponse/whitepapers/ransomware-a-growing-menace.pdf (describing ransomware—i.e., malware that locks a target's computer and requires payment of a fine as a condition of unlocking the computer—and "conservatively" estimating that over $5 million per year is being extorted from ransomware victims).

137. *Cybercrime*, INTERPOL, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (last visited Apr. 1, 2013) ("Cybercrime is one of the fastest growing areas of crime."). Some of our most personal information is now available on the thriving black market for a mere pittance. *How Much Do You Cost on the Black Market?*, OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., http://www.ncix.gov/issues/cyber/identity_theft.php (last visited Apr. 1, 2013) ("[On the black market,] [y]our social security number, at $3, is less expensive than a McDonald's Happy Meal.").

when you factor in downtime),[138] and a highly controversial McAfee estimate places cybercrime losses as high as $1 trillion in 2010 alone.[139]

2. Professionalization and Commoditization of Cybercrime

Cybercriminals have grown increasingly sophisticated, both in terms of business models[140] and in terms of tools,[141] leading cybercrime experts to warn that we have entered an era of cybercrime "professionalization" and

138. Press Release, Symantec, Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually (Sept. 7, 2011), *available at* http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (describing the methodology for arriving at the $114 billion and $388 billion figures as "extrapolations" based on a survey of over 12,000 adults conducted in twenty-four countries).

139. *See* Robert Richardson, *Bigger Than a Trillium*, COMPUTER SEC. INST., http://gocsi.com/public/trillium (last visited Apr. 1, 2013) (explaining that the $1 trillion estimate comes not from a McAfee report, but from company talking points); *Keith Alexander's Remarks*, *supra* note 74, at 09:29 ("McAfee estimates that $1 trillion was spent globally on remediation."); *see also* President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/video/President-Obama-on-Cybersecurity#transcript (citing McAfee's estimate of $1 trillion in cybercrime losses). *But see* Andy Greenberg, *McAfee Explains the Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim*, FORBES (Aug. 3, 2012), http://www.forbes.com/sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim/ (questioning the validity of the $1 trillion estimate, which McAfee has called a "ballpark figure" and "unscientific," but noting that McAfee stands by the estimate, saying that it was not simply made up); Peter Maas & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012, 11:12 AM), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (criticizing the validity of the $1 trillion estimate and reporting that Ross Anderson, a well-known security researcher at the University of Cambridge, called the "intellectual quality" of the $1 trillion estimate "below abysmal"). *See generally* ROSS ANDERSON ET AL., MEASURING THE COST OF CYBERCRIME (June 26, 2012), http://lyle.smu.edu/~tylerm/weis12pres.pdf (calling existing cybercrime estimates "eye-poppingly large," identifying methodological flaws in certain reports on costs of cybercrime, and offering a framework for analyzing the costs of cybercrime).

140. *See* TRENDMICRO, THE BUSINESS OF CYBERCRIME: A COMPLEX BUSINESS MODEL 5 (2010), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf ("[C]yber scams are often part of an intricate, highly sophisticated and highly organized [cybercrime] business model based on the concept of affiliate marketing."); Jim Finkle, *Inside a Global Cybercrime Ring*, REUTERS (Mar. 24, 2010, 11:12 AM), http://www.reuters.com/article/2010/03/24/us-technology-scareware-idUSTRE62N29T20100324 (describing Innovative Marketing, a "complex underground corporate empire with [cybercrime] operations stretching from Eastern Europe to Bahrain; from India and Singapore to the United States" with estimated revenue of about $180 million in 2008, as a "scareware" pioneer whose programs "pretend to scan a computer for viruses and then tell the user that their machine is infected" in order to scam users into paying to clean their PCs).

141. *See, e.g.*, Rachael King, *Operation High Roller Targets Corporate Bank Accounts*, WALL ST. J. CIO J. (June 26, 2012, 9:07 PM), http://blogs.wsj.com/cio/2012/06/26/operation-high-roller-targets-corporate-bank-accounts/ ("Operation High Roller is characterized by extensive automation.").

"commoditization of attack codes."[142]

With respect to the "professionalization" of cybercrime, there is substantial evidence that cybercriminals are adopting "time-tested business processes to enhance the profitability of crime syndicates worldwide."[143] As one journalist explains:

> The disturbing trend in cybercrime is the "enterprise-class" approach crime syndicates take to grow their businesses. Today's syndicates employ hierarchies of participants with roles that mirror the executive suite, middle management and the rank and file. The executive suite oversees strategy and operations that initiate nefarious acts. Recruiters identify "infantry" that carry out large-scale attack schemes on a permanent hire or outsource (affiliate) basis. They also . . . mold reward programs to pay affiliates once successful attacks are carried out . . . . [W]ith creative profit-sharing flair, crime syndicates are continuing to grow sophisticated pay-per-click/install/purchase affiliate programs to reward up and coming cybercriminal affiliates on a performance-based scale. [And] taking a page out of Wall Street, crime syndicates are engaging in mergers and acquisitions to grow their botnets . . . .[144]

Simultaneously, we are witnessing the commoditization of cybercrime tools. While hacking once required considerable technical expertise, cybercrime toolkits are now available as commodities on the black market,[145] as are so-called "zero-day" exploits, which are used to exploit

---

142. Tom Kellermann, Panel 1: The Promise and Peril of Being Interconnected, Interoperable, and Intelligent at the American University Law Review Symposium: America the Virtual: Security, Privacy, and Interoperability in an Interconnected World (Oct. 25, 2012), *available at* http://www.aulawreview.com/index.php?view=vidlink&catid=1:symposium-2012&id=155:promise-and-peril-of-interconnectivity&option=com_vidlinks&Itemid=150 ("You no longer need to learn to build a gun to learn to pull the trigger . . . [adversaries] don't have to build an AK-47; they just need to learn to use it.").

143. Derek Manky, *Why Cybercrime Remains Big Business – And How to Stop It*, FORBES (Feb. 1, 2013, 5:07 PM), http://www.forbes.com/sites/ciocentral/2013/02/01/why-cybercrime-remains-big-business-and-how-to-stop-it/.

144. *Id.* (describing how competition between two rival crimeware kits—Zeus and SpyEye—hurt profits for both, leading the botnet owners to "merge[] source code, retire[] Zeus support, and pass[] the torch to SpyEye.").

145. *See id.* ("Zeus, circa 2007, peaked in 2010 as the most prolific banking crime kit around. The crimeware kit would create new versions of powerful malware which had the capability to steal banking credentials, as well as hijack and manipulate secure online banking sessions."); RSA, RSA 2012 CYBERCRIME TRENDS REPORT: THE CURRENT STATE OF CYBERCRIME AND WHAT TO EXPECT IN 2012 (2012), http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf ("The more savvy criminals offer their goods and services to those who may be starting out or are in need of set-up and instructions. Whether selling off-the-shelf botnets, Trojans by the binary, or Zeus recompiles, the underground is loaded with tools to allow any 'newbie' cybercriminal to launch an attack.").

previously unknown vulnerabilities.[146] The black market demand for such exploits is driven by those who lack the "technical sophistication to find their own vulnerabilities and launch attacks," and the black market functions relatively efficiently with "Google-like search engines connect[ing] those who have discovered the vulnerability with customers who have the money to buy the knowledge," whether nation-states, criminals, terrorists, or hacktivists.[147]

B. Cyberespionage

> *Every major company in the United States has already been penetrated by China.*
> *-Richard Clarke, former White House counterterrorism expert and special advisor on cybersecurity to President Clinton*[148]

"Cyberespionage" in this Article refers to state-sponsored theft of industrial and defense secrets and/or intellectual property.[149] General Keith Alexander, who is dual-hatted as director of the NSA and chair of U.S. Cyber Command,[150] recently characterized the volume of intellectual

---

146. Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012, 9:40 AM), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ (documenting the black market for so-called "zero-day" exploits or "cyberweaponry"); Stew Magnuson, *Growing Black Market for Cyber-Attack Tools Scares Senior DoD Official*, NAT'L DEF. MAGAZINE (Feb. 22, 2013, 2:49 PM), http://www.nationaldefensemagazine.org/blog /Lists/Posts/Post.aspx?ID=1064 ("There has been a black market for those willing to sell knowledge of [zero-day exploits] for years. That market has now moved into the world of supervisory control and data acquisition (SCADA) systems that run power plants," according to Eric Rosenbach, deputy assistant secretary of defense for cyber policy).

147. Magnuson, *supra* note 146 ("[The] growing black market for zero-day vulnerabilities is allowing almost anyone with the cash to buy the means to launch destructive cyber-attacks against U.S. industrial control systems . . . .").

148. Ron Rosenbaum, *Richard Clarke on Who Was Behind the Stuxnet Attack*, SMITHSONIAN MAG. (Apr. 2012), http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html?c=y&story=fullstory.

149. *See* Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyberwar?*, THE NEW YORKER (Nov. 1, 2010), http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

150. Cyber Command, or CYBERCOM, "coordinates defense of the military part of the Internet, the '.mil' domain, and conducts offensive computer network operations as ordered." SPADE, *supra* note 23, at 28. *See U.S. Cyber Command Factsheet*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command/ (last updated Dec. 2011) ("USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while

property theft the United States experiences as "astounding"[151] and publicly stated that, in his opinion, it is the "greatest transfer of wealth in history."[152]

Some prominent examples of cyberespionage include: Moonlight Maze (1998);[153] Byzantine Hades (2002);[154] Operation Titan Rain (2003);[155]

---

denying the same to our adversaries."); *see also* Joanna Stern & Luis Martinez, *Pentagon Cyber Command: Higher Status Recommended*, ABC NEWS (May 2, 2012), http://abcnews.go.com/Technology/pentagon-cyber-command-unit-recommended-elevated-combatant-status/story?id=16262052#.UMU444QgqY.

151. *Keith Alexander's Remarks*, *supra* note 74, at 34:30.

152. *Id.* at 09:06-09:11. Cybersecurity expert Dmitri Alperovitch, the Chief Technology Officer of CrowdStrike, Inc., appears to have coined this phrase in August 2011 while working as Vice President of Threat Research at McAfee, Inc. *See* ALPEROVITCH, *supra* note 96, at 2 ("What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth—closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, supervisory control and data acquisition (SCADA) configurations, design schematics, and much more has 'fallen off the truck' of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries."); *see also* Dean Takahashi, *Black Hat's Spotlight Falls on McAfee's Dmitri Alperovitch for Uncovering Cyberspying*, VENTURE BEAT (Aug. 4, 2011, 7:00 AM), http://venturebeat.com/2011/08/04/black-hats-spotlight-falls-on-mcafees-dmitri-alperovitch-for-uncovering-cyber-spying/ (quoting Alperovitch, who called the widespread, China-based "Shady RAT" cyberespionage campaign the "biggest transfer of wealth in terms of intellectual property in human history").

153. Moonlight Maze refers to a series of intrusions into the U.S. Department of Defense ("DoD") computers that began in March 1998 and lasted for three years. Moonlight Maze probed computers at NASA, the Pentagon, the Department of Energy, and private institutions, accessing "troop configurations, maps of military installations, and military hardware designs" in what was then deemed the "largest sustained cyber-attack on the United States." Jessica Bourquin, The Evolution of Cyber Espionage: A Case for an Offensive U.S. Counterintelligence Strategy 11 (Oct. 14, 2011) (unpublished student white paper), *available at* https://www.treadstone71.com/index.php/news-info-whitepapers/masters-in-cybersecurity-intelligence-and-forensics/doc_download/48-the-evolution-of-cyber-espionage-jessica-bourquin. Experts traced the attacks to Moscow but could not confirm that Russia was responsible for the attacks. *Id.* at 12.

154. Byzantine Hades refers to a decade-long series of attacks believed to be perpetrated by the Chinese military. Brian Grow & Mark Hosenball, *Special Report: In Cyberspy vs. Cyberspy, China Has the Edge*, REUTERS (Apr. 14, 2011, 3:52 PM) http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414 ("Secret U.S. State Department cables, obtained by WikiLeaks and made available to Reuters by a third party, trace systems breaches – colorfully named "Byzantine Hades" by U.S. investigators – to the Chinese military. An April 2009 cable even pinpoints the attacks to a specific unit of China's People's Liberation Army.") These attacks, which generally rely on spear-phishing, have resulted in the exfiltration of terabytes of sensitive information from the U.S. government and private sector companies, including "designs for multi-billion dollar weapons systems," see id., such as the blueprints for the "quiet electric drive" that U.S. submarines use for stealth operation. Bourquin, *supra* note 153, at 13; Mathew J. Schwartz, *Leaked Cables Indicate Chinese Military Hackers Attacked U.S.*,

Operation Buckshot Yankee (2008);[156] Operation Night Dragon (2008–2011);[157] Operation Aurora (2009);[158] penetration of Lockheed Martin,

---

INFORMATIONWEEK (Apr. 19, 2011, 1:09 PM), http://www.informationweek.com/security/attacks/leaked-cables-indicate-chinese-military/229401866; Michael Riley and John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG (Dec. 14, 2011, 8:47 AM), http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html.

155. "Operation Titan Rain" refers to a series of security breaches that targeted sensitive, but unclassified information. The Department of Defense "has acknowledged that the majority of such incidents . . . were orchestrated by China as a method of cyber-espionage." Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 829 (2012). Beginning in 2003, the Titan Rain cyberespionage team successfully exfiltrated sensitive information from DoD as well as private sector companies supporting the military's mission. Exfiltrated data included copies of U.S. Air Force flight-planning software, "specifications for the aviation-mission-planning system used in Army helicopters," and "hundreds of detailed schematics on propulsion systems." Bourquin, *supra* note 153, at 15.

156. In 2008, DoD "suffered a significant compromise of its classified military computer networks." Melissa E. Hathaway, *Leadership and Responsibility for Cybersecurity*, GEO. J. OF INT'L AFF. (2012), at 71, 72. Specifically, Central Command, which was overseeing the wars in Iraq and Afghanistan, was penetrated through an infected USB drive. "Operation Buckshot Yankee" was the codename for recovery from this incident. *Id.*

157. "Night Dragon" is the code name for a cyberespionage campaign leveled against six global oil, energy, and petrochemical companies, including Exxon Mobil, Royal Dutch Shell, and BP. The attack has been described as a "systemic long-term compromise of [the] Western oil and gas industry." ALPEROVITCH, *supra* note 96, at 2. It is believed to have lasted from 2008 to 2011, during which time Chinese cyberspies are alleged to have stolen valuable intellectual property including: bidding information, prospecting data including computerized topographical maps worth "millions of dollars" that show locations of potential oil reserves, and highly sensitive confidential business information. Michael Riley, *Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers*, BLOOMBERG (Feb. 24, 2011, 3:26 AM), http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html. The tools, techniques, and network activities associated with the attack were traced back to China. ALPEROVITCH, *supra* note 96, at 2.

158. "Operation Aurora" refers to a successful Chinese cyberespionage campaign against Google and thirty-three other major U.S. companies (reportedly including Intel, Dow Chemical, Morgan Stanley, and computer security guru, Symantec). While reports initially suggested that the cyberspies were trying to hack primarily into Gmail accounts of Chinese dissidents as part of an effort to quell dissent, security experts later opined that the cyberspies were in fact targeting Google's sensitive systems and intellectual property. David Drummond, *A New Approach to China*, GOOGLE PUB. POL'Y BLOG (Jan. 12, 2010, 6:53 PM), http://googlepublicpolicy.blogspot.com/2010/01/new-approach-to-china.html. Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, (Nov. 28, 2010), http://www.nytimes.com/2010/11/29/world/29cables.html (reporting that leaked American diplomatic cables indicate that "China's Politburo directed the intrusion into Google's computer systems," and that the "Google hacking was part of a coordinated campaign of computer sabotage carried out [in part] by government operatives").

BAE Systems and Northrop Grumman (2009);[159] Operation Shady RAT (2006);[160] GhostNet (2009);[161] the RSA Breach (2011);[162] and twenty-three natural gas pipeline operators (December 2011–June 2012).[163]

---

159. Chinese cyberspies are alleged to have stolen several terabytes of classified data related to the design and electronics system of the F-35 Joint Strike Fighter, the Pentagon's $300 billion weapons project. Specifically, in 2009, cyberspies attacked networks belonging to several major western defense contractors, including Lockheed Martin and Northrop Grumman in the United States and BAE Systems in the United Kingdom. *See* Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009), http://online.wsj.com/article/SB124027491029837401.html.

160. "Operation Shady RAT" refers to a five-year cyberspying campaign allegedly perpetrated by the Chinese that successfully penetrated the computer networks of more than seventy governments and major corporations (including thirteen defense contractors) in fourteen countries. Approximately fifty targets were in the United States. The list of governments and institutions believed to have been infiltrated includes the United States, Taiwan, Vietnam, Canada, the United Nations, the Olympic committees in three countries, and the International Olympic Committee. *See* ALPEROVITCH, *supra* note 96, at 2–4; Takahashi, *supra* note 152.

161. GhostNet refers to a "vast" malware-based cyberespionage network exposed in 2009 that penetrated more than 1200 computer systems in 103 countries. RON DIEBERT & RAFAL ROHOJINSKI, TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK, INFORMATION WARFARE MONITOR 5 (Mar. 29, 2009), http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; *see* John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES (Mar. 28, 2009), http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all&gwh=0F9A5B2A394E6EF2A8B207B0D8305565. The GhostNet remote access tool may have been created by the same organization as Byzantine Hades. Bourquin, *supra* note 153, at 13.

162. RSA Security's products protect computer networks at the White House, CIA, NSA, Pentagon, Department of Homeland Security ("DHS"), most top defense contractors, and the majority of Fortune 500 companies. RSA is best known for the SecurID key fob that forty million employees across the globe use to remotely access their employer's computer networks. In May 2011, hackers breached the servers at RSA and stole information that could be used to compromise the security of the fobs used to access sensitive corporate and government networks. Chinese hackers are believed to have targeted RSA in order to compromise defense contractors and government agencies using RSA's technology, a view borne out by the fact that shortly after the attack on RSA, Lockheed Martin was attacked using information gained from the RSA attack. *See* Siobhan Gorman & Shara Tibken, *Security 'Tokens' Take Hit*, WALL ST. J. (June 7, 2011), http://online.wsj.com/article/SB10001424052702304906004576369990616694366.html ("[RSA Security] openly acknowledged for the first time that intruders had breached its security systems at defense contractor Lockheed Martin Corp. using data stolen from RSA."). The subsequent investigation revealed that hackers used spearphishing (described at *supra* note 84) to gain access to RSA's servers.

163. Clayton, *supra* note 118 ("Cyberspies linked to China's military targeted nearly two dozen U.S. natural gas pipeline operators over a recent six-month period, stealing information that could be used to sabotage U.S. gas pipelines.").

1. Costs of Cyberespionage

By some reports, cyberespionage is estimated to cost the United States (in terms of lost jobs, innovation, and national security) and its corporations (in terms of lost intellectual property, remediation, and reduced consumer confidence) up to $200 billion annually,[164] but reliably quantifying the potentially staggering costs of cyberespionage has been an elusive goal. Obstacles include the fact that many companies do not know that they have been victimized and even those that do know are often reluctant to disclose out of concern for their reputation. Moreover, "victims of trade secret theft use different methods to estimate their losses; some base estimates on the actual costs of developing the stolen information, while others project the loss of future revenues and profits."[165]

2. Advanced Persistent Threats

One particularly insidious form of cyberespionage is known as an advanced persistent threat ("APT"). APTs are highly targeted malware-based attacks[166] with several distinguishing features. First, as their name suggests, APTs are often—though not always—advanced.[167] In many cases, they "utilize the full spectrum of computer intrusion technologies and techniques" and "combine multiple attack methodologies and tools in order to reach and compromise their target."[168] Second, APTs are

164. J. P. London, *Made In China*, 137 U.S. NAVAL INST. PROCEEDINGS MAG. (Apr. 2011), http://www.usni.org/magazines/proceedings/2011-04/made-china#footnotes ("Cyber espionage alone is estimated to cost the United States up to $200 billion a year."); *see* Mike McConnell et al., *China's Cyber Thievery is National Policy—And Must Be Challenged*, WALL ST. J. (Jan. 27, 2012), http://www.boozallen.com/media/file/WSJ-China-OpEd.pdf ("[I]t is also difficult to estimate the economic costs of [cyberespionage] . . . to the U.S. . . . [but] we think it is safe to say that [it is] . . . billions of dollars and millions of jobs.").

165. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE i (2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [hereinafter NCIX, FOREIGN SPIES].

166. *See What is Malware?*, MICROSOFT SAFETY & SEC. CTR., http://www.microsoft.com/security/resources/malware-whatis.aspx (last visited Apr. 1, 2013) ("Malware is any kind of unwanted software that is installed without your adequate consent.").

167. *Contra* Kelly Jackson Higgins, *Government Agencies Get Creative in APT Battle*, DARK READING (Oct. 3, 2012, 7:31 PM), http://www.darkreading.com/threat-intelligence/167901121/security/news/240008438/government-agencies-get-creative-in-apt-battle.html (quoting Australian cybersecurity expert David Cottingham, who asserts that APTs are "not actually that advanced at all" and are more like "targeted, persistent threats").

168. *Advanced Persistent Threats (APT)*, DAMBALLA, https://www.damballa.com/knowledge/advanced-persistent-threats.php (last visited Apr. 1, 2013).

persistent.[169] APT operators seek long-term access to their targets, with attack objectives generally extending beyond immediate financial gain.[170] In order to maintain long-term access to targets, APTs generally operate stealthily for as long as possible.[171] Finally, APTs rely on "skilled, motivated, organized and well-funded" operators to coordinate and execute attacks.[172] The substantial resources required to operate APTs generally makes them a tool of nation-states. At their essence, APTs are "computer intrusions staged by threat actors that aggressively pursue and compromise specific targets, often leveraging social engineering or the 'art of manipulation,' in order to maintain a persistent presence within the victim's network so that they can move laterally and extract sensitive information."[173]

APTs traditionally targeted government and military networks.[174] Now, they also target "the defense industrial base and high tech companies, the energy and finance sectors, telecommunications companies as well as media outlets, civil society organizations and academic institutions."[175] Law firms and other small- and medium-sized businesses that work with large companies increasingly are being targeted because they often are entrusted with clients' most sensitive information, yet have weaker cyber defenses.[176]

---

169. Press Release, Mandiant, Mandiant Releases Annual Threat Report on Advanced Targeted Attacks, Mar. 13, 2013, *available at* https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks1/ ("Attackers spend an estimated 243 days on a victim's network before they are discovered.").

170. DAMBALLA, *supra* note 168.

171. *See* Higgins, *supra* note 167 ("Cyberespionage attacks are often camouflaged to maintain their foothold in the victim's network."); DAMBALLA, *supra* note 168 ("[O]perators of APT technologies tend to focus on 'low and slow' attacks—stealthily moving from one compromised host to the next, without generating regular or predictable network traffic—to hunt for their specific data or system objectives. Tremendous effort is invested to ensure that malicious actions cannot be observed by legitimate operators of the systems.").

172. DAMBALLA, *supra* note 168.

173. *Developments in China's Cyber and Nuclear Capabilities: Hearing Before the U.S.-China Econ. and Security Rev. Comm'n*, 112th Cong. 29 (2012) [hereinafter *Devs. in China's Cyber and Nuclear Capabilities*] (statement of Nart Villeneuve, Senior Threat Researcher, TrendMicro), http://origin.www.uscc.gov/sites/default/files/transcripts/3.26.12HearingTranscript.pdf.

174. *Id.* at 31.

175. *Id.* at 29.

176. *Think That Cyber Espionage Only Happens to Big Companies? Think Again. Hackers Are Targeting Smaller Companies*, RDINSIGHTS (Nov. 5, 2012), http://www.rdinsights.com/2012/11/think-that-cyber-espionage-only-happens-to-big-companies-think-again-hackers-are-targeting-smaller-companies-vendors-and-suppliers/ (asserting that small- and medium-sized businesses have weaker cybersecurity measures "in terms of infrastructure and personnel training" and noting

APTs are likely to remain one of the most serious concerns for U.S. businesses for some years to come,[177] but with the explosive growth of mobile broadband and cloud computing, experts are warning that mobile-malware,[178] including mobile "drive-by-downloads,"[179] and cloud-based attacks[180] may be the "next big thing."

3. Cyberespionage Implications

Regardless of the type of attack and specific attack vector,[181] cyberespionage poses a serious threat to U.S. economic and national security. On the national security side, cyberespionage has been dubbed "the biggest intelligence disaster since the loss of nuclear secrets [in the late 1940s]."[182] Perpetrators "not only gather[] information, but can map networks for future attacks and can leave behind backdoors or malware

---

that without "on-going security auditing" smaller companies may not know if they were hacked or how much client information has been compromised).

177. *Kaspersky Lab Predicts Core Threats for 2013*, NET SEC. (Dec. 6, 2012), http://www.net-security.org/secworld.php?id=14072 ("Kaspersky Lab expects . . . targeted attacks, with the purpose of cyber-espionage, to continue in 2013 and beyond, becoming the most significant threat for businesses.").

178. ESET, TRENDS FOR 2013: ASTOUNDING GROWTH OF MOBILE MALWARE 2 (2012), http://go.eset.com/us/resources/white-papers/Trends_for_2013_preview.pdf ("[W]e see as the main trend for 2013 an exponential growth of mobile malware."); TRENDMICRO, SECURITY THREATS TO BUSINESS, THE DIGITAL LIFESTYLE, AND THE CLOUD: TREND MICRO PREDICTIONS FOR 2013 AND BEYOND 1 (2012), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp-trend-micro-predictions-for-2013-and-beyond.pdf ("The volume of malicious and high-risk Android apps will hit 1 million in 2013.").

179. *See* VERIZON, *supra* note 91, at 27 (explaining that drive-by downloads are auto-executed web-based malware); *Drive-By Downloads: How They Attack and How to Defend Yourself*, TECHNEWSDAILY (May 18, 2012, 9:01 AM), http://www.technewsdaily.com/7789-driveby-download-definition.html ("Drive-by downloads are malicious pieces of software that are downloaded to a computer, tablet or smartphone when the user views a compromised Web page or HTML-based email message. In many cases, the malware will be automatically installed on the system.").

180. NET SEC., *supra* note 177 ("[2013 will bring an] increase in cybercriminal attacks targeting cloud-based services.").

181. An attack vector is the technical term used by cybersecurity experts to describe "the approach used to assault a computer system or network." *Attack Vector*, PC MAG., http://www.pcmag.com/encyclopedia_term/0%2C1237%2Ct%3Dattack+vector&i%3D57711%2C00.asp (last visited Apr. 1, 2013).

182. *War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?*, ECONOMIST (July 1, 2010), http://www.economist.com/node/16478792 (quoting James Lewis at CSIS); *see* Letter from Michael Chertoff et al. to Harry Reid & Mitch McConnell, U.S. Senators (June 6, 2012), *available at* http://www.hsgac.senate.gov/download/cybersecurity-support-letter-from-top-national-security-leaders ("[The cyberthreat] represents one of the most serious challenges to our national security since the onset of the nuclear age sixty years ago.").

designed to execute or facilitate [a future] attack."[183] With respect to the implications of cyberespionage for economic security, Richard Clarke, the former counterterrorism czar in three U.S. presidential administrations, recently offered this grim warning:

> Every major company in the United States has already been penetrated by China.
>
> . . . .
>
> My greatest fear . . . is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese. And we never really see the single event that makes us do something about it. That it's always just below our pain threshold. That company after company in the United States spends millions, hundreds of millions, in some cases billions of dollars on R&D and that information goes free to China . . . . After a while you can't compete.[184]

4. Perpetrators of Cyberespionage

Many countries—including Russia, France, Israel, India, Japan, and Taiwan—are believed to engage in cyberespionage,[185] but according to most cybersecurity experts, China is in a class by itself.[186] China has both the ability and the motivation to engage in a campaign of cyberespionage,[187] given the close relationship between China's military

183. SPADE, *supra* note 23, at 7.

184. Rosenbaum, *supra* note 148; *see* ALPEROVITCH, *supra* note 96, at 3 ("[I]f even a fraction of [the petabytes of exfiltrated data] is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat not just to individual companies and industries but to entire countries that face the prospect of decreased economic growth in a suddenly more competitive landscape and the loss of jobs in industries that lose out to unscrupulous competitors in another part of the world. And let's not forget the national security impact of the loss of sensitive intelligence or defense information.").

185. Hersh, *supra* note 149 ("[According to a] retired four-star Navy admiral . . . Russia, France, Israel, and Taiwan conduct the most cyber espionage against the U.S."); *see also* U.S. DEP'T OF DEF., *supra* note 23, at 6–7 ("Espionage has a long history and is nearly always practiced in both directions. For the U.S. and many other states, traditional espionage has been a state-sponsored intelligence-gathering function focused on national security, defense, and foreign policy issues. The United States Government collects foreign intelligence via cyberspace, and does so in compliance with all applicable laws, policies, and procedures. The conduct of all U.S. intelligence operations is governed by long-standing and well-established considerations, to include the possibility those operations could be interpreted as a hostile act.").

186. U.S.-CHINA ECON. & SEC. REV. COMM'N, 2012 REPORT TO CONGRESS 155 (2012), http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf.

187. *See* Stuart Fox, *Hacker Attacks on US Reveal China's Weakness*,

and its state-owned companies;[188] the lack of independent research and development in China;[189] and the state of the Chinese economy.[190] Chinese actors are considered "the world's most active and persistent perpetrators of economic espionage," according to a 2011 National Counterintelligence Executive Report to Congress,[191] and cyberespionage is believed to be an important component of China's long-term economic development strategy.[192] According to three former high-ranking U.S. government officials—the former Director of National Intelligence, Secretary of Homeland Security, and Deputy Secretary of Defense—"[t]he Chinese government has a national policy of economic espionage in cyberspace."[193]

TECHNEWSDAILY (Jan. 11, 2012, 4:32 PM), http://www.technewsdaily.com/7457-chinese-hacking-espionage-weakness.html.

188. *See* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 186, at 156 ("The state controls up to 50 percent of the Chinese economy, and industrial espionage appears to be a key mission of the Chinese intelligence services."); *see also* REP. MIKE ROGERS & REP. DUTCH RUPPERSBERGER, H. PERMANENT SELECT COMM. ON INTELLIGENCE, 112TH CONG., INVESTIGATIVE REP. ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE iv (Comm. Print 2011), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (warning U.S. companies and government agencies not to do business with China's Huawei and ZTE, the world's second and fifth largest manufacturers of routers, based on concerns about supply chain security).

189. *See, e.g.*, Michael A. Riley & Ashlee Vance, *China Corporate Espionage Boom Knocks Wind out of U.S. Companies*, BLOOMBERG (Mar. 15, 2012), http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html (paraphrasing Harvard Business School professor Willy Shih's comments that the Chinese "need to build a research and development culture that can supersede their skills at mimicry"); *China's Pharmaceutical Industry Lacks Innovation, Lags Behind*, WORLDWATCH INST., http://www.worldwatch.org/node/3923 (last visited Feb. 18, 2013) ("China's pharmaceutical industry still lacks independent and efficient research and development capabilities . . . ."). *See generally* McConnell et al., *supra* note 164.

190. McConnell et al., *supra* note 164 ("China has a massive, inexpensive work force ravenous for economic growth.").

191. NCIX, FOREIGN SPIES, *supra* note 165, at i; *see* McConnell et al., *supra* note 164 ("Evidence indicates that China intends to help build its economy by intellectual-property theft rather than by innovation and investment in research and development . . . .").

192. Siobhan Gorman, *China Singled Out for Cyberspying*, WALL ST. J. (Nov. 4, 2011), http://online.wsj.com/article/SB10001424052970203716204577015540198801540.html (according to a senior intelligence official, "economic espionage is condoned by both China and Russia and is part of each country's national economic development policy"); KREKEL ET AL., *supra* note 23, at 107 ("The apparent expansion of China's computer network exploitation (CNE) activities to support espionage has opened rich veins of previously inaccessible information that can be mined both in support of national security concerns and, more significantly, for national economic development.").

193. McConnell et al., *supra* note 164; *see* NCIX, FOREIGN SPIES, *supra* note 165, at 5 (accusing not only China, but also Russia of using cyberespionage to steal U.S.

Although China repeatedly has denied involvement in cyberespionage,[194] there is extensive evidence tying China to cyberespionage campaigns.[195] First, and most obviously, U.S. companies have reported numerous Chinese attempts to steal "client lists, merger and acquisition data, pricing information, and the results of research and development efforts."[196]

Second, the 2013 National Intelligence Estimate ("NIE"), a classified document reflecting the "consensus view of the U.S. intelligence community,"[197] reportedly concluded that "the United States is the target of a massive, sustained cyber-espionage campaign that is threatening the country's economic competitiveness."[198] According to press reports based on interviews of individuals familiar with the report, the NIE identified China "as the country most aggressively seeking to penetrate the computer systems of American business and institutions."[199]

---

industrial secrets as a matter of national policy).

194. In January 2013, the Chinese Defense Ministry stated: "It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence," and in February 2013, Chinese Ministry of Foreign Affairs spokesman HongLei asserted: "China resolutely opposes hacking actions and has established relevant laws and regulations and taken strict law enforcement measures to defend against online hacking activities." David E. Sanger et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html; *see* Thom Shanker, *U.S. Report Accuses China and Russia of Internet Spying*, N.Y. TIMES (Nov. 3, 2011), http://www.nytimes.com/2011/11/04/world/us-report-accuses-china-and-russia-of-internet-spying.html ("[Chinese] Foreign Ministry spokesman Hong Lei said, 'The Chinese government opposes hacking in all its manifestations.' ").

195. *See, e.g.*, NCIX, FOREIGN SPIES, *supra* note 165, at 5; KREKEL ET AL., *supra* note 23, at 100; Michael Riley & Dune Lawrence, *Hackers Linked to China's Army Seen From EU to D.C.*, BLOOMBERG (July 26, 2012, 7:00 PM), http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html; *see also*, *supra* notes 157–162.

196. Mike Brownfield, *Morning Bell: Stopping the Cyber Espionage Threat*, THE FOUNDRY (Apr. 26, 2012, 9:06 AM), http://blog.heritage.org/2012/04/26/morning-bell-stopping-the-cyber-espionage-threat/.

197. Ellen Nakashima, *U.S. Said To Be Target of Massive Cyber-Espionage Campaign*, WASH. POST (Feb. 10, 2013), http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets ("Some officials have pressed for an unclassified version of the report to be released publicly, [but] . . . as a matter of policy, [the Office of the Director of National Intelligence does] not discuss or acknowledge the existence of NIEs unless directed to do so.").

198. *Id.*

199. *Id.*; *see* David Barboza, *In Wake of Cyberattacks, China Seeks New Rules*, N.Y. TIMES (Mar. 10, 2013), http://www.nytimes.com/2013/03/11/world/asia/china-calls-for-global-hacking-rules.html ("American intelligence officials have [] said privately that they have evidence of Chinese government involvement in the [recent hacking] attacks.").

Third, just days after the NIE was circulated, U.S. information security company Mandiant released a report of over sixty pages offering extensive evidence of Chinese espionage,[200] including actual video of intrusion activities in action.[201] Based on this evidence, Mandiant said that it believes that since at least 2006, Unit 61398 of China's People's Liberation Army[202] has been conducting an extensive cyberespionage campaign that has resulted in the exfiltration of hundreds of terabytes of data—including "broad categories of intellectual property [such as] technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and e-mails and contacts lists from victim organizations' leadership"—from over 140 companies in twenty major industries.[203] Although not without its critics both in the United States[204] and beyond its borders,[205] the February 13, 2013 Mandiant Report is notable for its public proffer of detailed evidence that China is engaged in extensive government-sponsored cyberespionage campaigns.

---

200. It should be noted that the group behind these attacks is "the same group that [Dmitri] Alperovitch [then Vice President of Threat Research for MacAfee] identified [in 2011]" as having perpetrated Operation Shady RAT. Jody Westby, *Mandiant Report on Chinese Hackers Is Not News But Its Approach Is*, FORBES (Feb. 20, 2013, 8:07 AM), http://www.forbes.com/sites/jodywestby/2013/02/20/mandiant-report-on-chinese-hackers-is-not-news-but-its-approach-is/. In 2011, Dmitri Alperovitch, then vice president of Threat Research for McAfee, authored a report about Shady RAT, the malware that had been used by Chinese cybercriminals to exfiltrate data from a broad cross-section of organizations over a two- to five-year period—undetected. Alperovitch broke new ground when he included a table of more than seventy companies, organizations, and government agencies from around the globe that had been compromised. *Id.*

201. MandiantCorp, *APT1: Exposing One of China's Cyber Espionage Units*, YOUTUBE (Feb. 18, 2013), http://www.youtube.com/watch?v=6p7FqSav6Ho (showing live APT1 Chinese threat actors, codenamed DOTAs, conducting computer network espionage activities).

202. PLA Unit 61398 is formally known as the Second Bureau of the People's Liberation Army General Staff Department's Third Department. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

203. *Id.* at 3.

204. *See* Mathew J. Schwartz, *China Denies U.S. Hacking Allegations: 6 Facts*, INFO. WEEK (Feb. 21, 2013, 11:40 AM), http://www.informationweek.com/security/attacks/china-denies-us-hacking-accusations-6-fa/240149058? (noting that Taia Global CEO Jeffrey Carr, who does not dispute that China engages in "massive amounts of cyber-espionage," believes that a more rigorous analysis of Mandiant's APT evidence (e.g., by a "professional intelligence analyst") "would likely have failed to prove attribution").

205. *See, e.g.*, *id.* (discussing Chinese media reports suggesting that the Mandiant report was a "commercial stunt" designed to sell information security products and services); *id.* (citing Chinese government comments describing the Mandiant report as "baseless").

5. Cyberespionage and U.S.-China Relations

Despite the potentially dire economic and national security implications of cyberespionage for the United States, it was only recently, in the face of mounting *public* evidence of the Chinese government's involvement in cyberespionage targeting U.S. companies, that the United States and China began the lengthy, but important, process of diplomatic engagement on the issue.

U.S. media reports of Chinese government-sponsored espionage intensified in the weeks after the Mandiant Report was issued, aggravating existing tensions between the United States and China on cybersecurity and prompting what some have referred to as a "war of words."[206] China's Foreign Minister Yan Jiechi said U.S. reports of Chinese government involvement in cyberespionage were "built on shaky ground" and that "[a]nyone who tried to fabricate or piece together a sensational story to serve a political motive will not be able to blacken the name of others nor whitewash themselves."[207] China increasingly went on the offensive, complaining that it is the victim of hack attacks linked to U.S. Internet Protocol addresses,[208] and the Chinese government repeatedly reasserted its official position that it opposes hacking.

Mounting tensions heightened concerns that U.S. accusations of Chinese cyberespionage would prompt trade-based retaliation from China. Indeed, just a few weeks after the *New York Times* identified Coca-Cola as having been the target of Chinese cyberespionage—in the same article that featured the Mandiant Report[209]—a remote Chinese provincial government announced that it is investigating Coca-Cola for "illegally collecting classified information with handheld GPS equipment."[210] The U.S. company, which is cooperating with the investigation, has denied any wrongdoing and says that it is simply using " 'location-based customer

206. Terril Yue Jones, *U.S., China agree to work together on cyber security*, REUTERS (Apr. 13, 2013, 11:37 AM), http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413.

207. Barboza, *supra* note 199.

208. *Id.* Jones, *supra* note 206 ("China claims it is the victim of large-scale cyber attacks from the United States").

209. Sanger et al., *supra* note 194. A few months earlier, the *New York Times* identified Coca-Cola as the likely unnamed victim of a cyberespionage campaign discussed in a 2010 case study published by Mandiant. Nicole Perlroth, *Study May Offer Insight Into Coca-Cola Breach*, N.Y. TIMES BITS BLOG (Nov. 30, 2012, 4:09 PM), http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/.

210. Patti Waldmeir, *Coca-Cola Probed over Mapping in China*, FIN. TIMES (Mar. 12, 2013, 3:43 PM), http://www.ft.com/intl/cms/s/0/f02a6abc-8b21-11e2-b1a4-00144feabdc0.html#axzz2PGMb8mqi.

logistics systems . . .' to improve customer service and fuel efficiency."[211] Regardless of what motivated the Coca-Cola investigation, many U.S. companies are concerned about the potential trade ramifications of confronting China on cyberespionage.

On the other hand, the increasingly public discussion of China's involvement in cyberespionage has not been without benefit. Several noteworthy diplomatic developments came about in the weeks and months following the release of the Mandiant Report. On March 10, 2013, approximately one month after the report was released, China's Foreign Minister took an important diplomatic step, calling for international " 'rules and cooperation' " on Internet espionage issues . . . ."[212] The following day, Tom Donilon, National Security Advisor to the President, delivered a speech to the Asia Society unequivocally setting forth the expectations of the U.S. with respect to China's role in cyberespionage. He said that building a constructive relationship with China is one of the pillars of the U.S. strategy in the Asia-Pacific region, and he identified cybersecurity as a "growing challenge to [the U.S.-China] economic relationship." Donilon said that U.S. cybersecurity concerns have "moved to the forefront of our agenda," and made clear that industrial cyberespionage was an animating concern,[213] stating:

> The international community cannot afford to tolerate such activity from any country. As the President said in the State of the Union, we will take action to protect our economy against cyber-threats. From the President on down, this has become a key point of concern and discussion with China at all levels of our governments. And it will continue to be. The United States will do all it must to protect our national networks, critical infrastructure, and our valuable public and private sector property. But, specifically with respect to the issue of cyber-enabled theft, we seek three things from the Chinese side. First, we need a recognition of the urgency and scope of this problem and the risk it poses—to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a

211. *Id.*

212. Barboza, *supra* note 199.

213. "I am not talking about ordinary cybercrime or hacking [and] this is not solely a national security concern or a concern of the U.S. government. Increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." Tom Donilon, Nat'l Sec. Advisor to the President, Address to the Asia Society: The United States and the Asia-Pacific in 2013 (Mar. 11, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

> constructive direct dialogue to establish acceptable norms of behavior in cyberspace . . . . [T]he United States and China, the world's two largest economies, both dependent on the Internet, must lead the way in addressing this problem.[214]

President Obama himself addressed the issue of nation-state sponsored cyberintrusions just two days later in a March 13 interview, stating: "[w]e've made it very clear to China...that, you know, we expect them to follow international norms and abide by international rules."[215] When newly elected Chinese President Xi Jinping took office on March 14, 2013, President Obama reportedly called to congratulate Xi and took the opportunity to raise U.S. concerns about hacking.[216] In the course of the call, the two leaders reportedly "committed to engage in an ongoing discussion to address the cyber issue."[217]

The conversation between Obama and Xi appears, at least momentarily, to have eased the war of words between China and the United States and to have accelerated formal diplomatic engagement on cybersecurity between the two countries. On March 17, 2013, just days after the Obama-Xi discussion, the new Chinese Premier Li Keqiang said: "I think we should not make groundless accusations against each other, and spend more time doing practical things that will contribute to cyber-security,"[218] and by mid-April 2013, U.S. Secretary of State John Kerry announced that the United States and China had agreed to set up a cybersecurity working group.[219]

While increased diplomatic engagement with China on cybersecurity is encouraging, substantive progress will take time, and, as the U.S. Under Secretary of State for Economic Affairs has noted: "It's important to have a dialogue on this, but it's also important that the dialogue be a means to an end and the end is really ending these practices."[220]

C. Cyberwar

The term "cyberwar" in this Article refers to "actions by a nation-state to penetrate another nation's computers or networks for the purposes of

---

214. *Id.*

215. Steve Holland, *Obama, China's Xi discuss cybersecurity dispute in phone call*, REUTERS (Mar. 14, 2013, 6:03 PM), http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314.

216. *Id.*

217. *Id.*

218. Terril Yue Jones, *China's new premier seeks "new type" of ties with U.S.*, REUTERS (Mar. 17, 2013, 4:02 AM), http://www.reuters.com/article/2013/03/17/us-china-parliament-hacking-idUSBRE92G02320130317.

219. Jones, *supra* note 206.

220. *Id.*

causing damage or disruption."[221] It is believed that "at least 12 of the world's 15 largest militaries are building cyberwarfare programs,"[222] with several nation-states—including the U.S.,[223] China,[224] Russia,[225] Israel,[226]

---

221. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010).

222. Scott Shane, *Cyberwarfare Emerges from Shadows for Public Discussion by U.S. Officials*, N.Y. TIMES (Sept. 26, 2012), http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html. *Cf.* Pierluigi Paganini, *The Rise of Cyberweapons and Relative Impact on Cyberspace*, INFOSEC INST. RESOURCES (OCT. 5, 2012), http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/ (noting that the number of nation-states developing cyberweapons reportedly is as high as 140).

223. Mark Mazzetti & David E. Sanger, *Security Leader Says U.S. Would Retaliate Against Cyberattacks*, N.Y. TIMES (Mar. 12, 2013), http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html ("[General Keith Alexander] told Congress [] that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks, the first time the Obama administration admitted to developing such weapons for use in wartime."). The U.S. government "has only recently acknowledged developing cyberweapons, and it has never admitted using them" despite "reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year." David E. Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (discussing what role the United States had in the development of the Stuxnet virus, which successfully destroyed centrifuges at a key Iranian nuclear enrichment facility beginning in 2008); *see* Leon E. Panetta, Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 ("[T]he Department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace."); U.S. DEP'T OF DEF., *supra* note 23, at 5 ("[T]he Department [of Defense] has the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests. If directed by the President, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict.").

224. *See generally* KREKEL ET AL., *supra* note 23.

225. *See* Bumiller & Shanker, *supra* note 107; Kim Hart, *Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar*, WASH. POST (Aug. 14, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html?sid=ST2008081303990 (discussing accusations that Russia launched cyberattacks against Georgia's Internet infrastructure, disabling many Georgian government websites and effectively establishing an "information blockade.").

226. *Israel Builds Up Its Cyberwar Corps*, UPI (Nov. 2, 2012, 2:37 PM), http://www.upi.com/Business_News/Security-Industry/2012/11/02/Israel-builds-up-its-cyberwar-corps/UPI-52421351881449/ ("Israeli Prime Minister Binyamin Netanyahu established a special division of Unit 8200 [the Israeli equivalent of the NSA] in 2010 to develop [Israel's] cyberwar capabilities."); *see* Sanger, *supra* note 223 (discussing Israel's role in the Stuxnet attack on Iran's nuclear enrichment facilities); *see also* John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES (Sept. 26, 2010),

North Korea,[227] and Iran[228]—already considered to have joined the ranks of the cyberwar-capable. As the "weaponization" of cyber accelerates, mainstream press reports of the cyberwar threat tend to highlight the potentially devastating effects of cyberattacks on our nation's critical infrastructure.[229] These reports describe, *inter alia*, how cyberattacks (1) on the power grid could lead to cascading failures across the nation with catastrophic consequences; (2) on financial systems could lead to economic panic and/or a crashing stock market; (3) on water systems could open dams causing flooding or make entire cities uninhabitable; (4) on rail systems (e.g., involving intentional misrouting of trains) could cause massive collisions; (5) on air-traffic control systems could lead to mass casualties; and (6) on nuclear facilities could result in a nuclear reactor meltdown, leading to catastrophic loss of life.[230] Nonetheless, exactly what constitutes a cyberattack remains ill-defined.

The U.S. military formally distinguishes between two types of offensive cyberpower available to nation-states: Cyber Network Exploitation ("CNE") and Cyber Network Attack ("CNA"). While CNE is essentially espionage, CNA refers to destructive attacks. Specifically, CNAs are

---

http://www.nytimes.com/2010/09/27/technology/27virus.html?hp&_r=0.

227. Tony Capaccio, *North Korea Improves Cyber Warfare Capacity, U.S. Says*, BLOOMBERG (Oct. 23, 2012, 12:45 AM), http://www.bloomberg.com/news/2012-10-23/north-korea-improves-cyber-warfare-capacity-u-s-says.html ("North Korea's government has a 'significant' cyber warfare capability that it continues to improve [according to] the top U.S. commander on the Korean Peninsula.").

228. Ellen Nakashima, *Iran Blamed for Cyberattacks on U.S. Banks and Companies*, WASH. POST (Sept. 21, 2012), http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html ("Iran recently has mounted a series of disruptive computer attacks against major U.S. banks and other companies in apparent retaliation for Western economic sanctions aimed at halting its nuclear program, according to U.S. intelligence and other officials.").

229. The devastating effects of a cyberattack are not necessarily limited to physical effects, but also may include economic and psychological effects (e.g., undermining confidence in systems). *See, e.g.*, SPADE, *supra* note 23, at 26 (noting that a one-day attack on American credit card companies has been estimated to cost $35 billion, and a "full-scale attack" on critical infrastructure could cost $700 billion).

230. *See, e.g.*, Bumiller & Shanker, *supra* note 107 ("An aggressor nation or extremist group could use . . . cyber tools to gain control of critical switches . . . . They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."); Robert Johnson, *New Cyber Attacks Will Target Power Grids and Major Public Works*, BUS. INSIDER (Sept. 14, 2011), http://articles.businessinsider.com/2011-09-14/news/30153012_1_data-theft-turbine-cyber-warfare; Barton Gellman, *Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Web as Tool of Bloodshed, Experts Say*, WASH. POST, June 27, 2002, at A1 ("U.S. analysts believe that by disabling or taking command of the floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real-world lives and property.").

defined as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[231]

We admittedly have come a long way since 2010 when U.S. Deputy Secretary of Defense William J. Lynn III said, "There's no agreed-on definition of what constitutes a cyberattack."[232] But an important debate continues to rage in military and national security law circles over what, precisely, qualifies as a cyberattack and/or an act of cyberwar[233] and the appropriate range of nation-state responses to such an act.[234] When it comes to an act of cyberwar, "it's in the eye of the beholder."[235]

In November of 2011, the U.S. Department of Defense ("DoD") concluded for the first time that cyberattacks can constitute an act of war[236] to which the United States may respond using traditional military force

---

231. JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 60 (2012), http://www.dtic.mil/doctrine/newpubs/jp102.pdf.

232. Cheryl Pellerin, *Lynn: Cyberspace is the New Domain of Warfare*, U.S. DEP'T OF DEF., AM. FORCES PRESS SERV. (Oct. 18, 2010), http://www.defense.gov/news/newsarticle.aspx?id=61310.

233. *See* Catherine Lotrionte, *Cyber Operations: Conflict Under International Law*, GEO. J. OF INT'L AFF. 15, 16 (2012) ("examin[ing] the challenges in defining the term cyberwar and [] propos[ing] a working definition . . . ."). *See generally* Hathaway et al., *supra* note 155.

234. For example, President Barack Obama's *International Strategy for Cyberspace* released in May 2011 marked the first time that the U.S. expressed the position that it would regard cyberattacks as on par with conventional attacks. *See* WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 28, at 14 ("When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."); *id.* ("We reserve the right to use all necessary means—diplomatic, informational, military and economic . . . in order to defend our Nation, our allies, our partners and our interests."). In a veiled reference to Article 5 of the NATO charter requiring allies to regard an attack against any member as an attack against all, the strategy stated: "we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners." *Id.*

235. Ellen Nakashima, *U.S. Cyber Approach 'Too Predictable' for One Top General*, WASH. POST (July 14, 2011), http://www.washingtonpost.com/national/national-security/us-cyber-approach-too-predictable-for-one-top-general/2011/07/14/gIQAYJC6EI_story.html (quoting a July 2011 comment made by General James Cartwright, former vice chairman of the Joint Chiefs of Staff).

236. U.S. DEP'T OF DEF., *supra* note 23, at 9 ("The phrase 'act of war' is frequently used as shorthand to refer to an act that may permit a state to use force in self-defense, but more appropriately, it refers to an act that may lead to a state of ongoing hostilities or armed conflict. Contemporary international law addresses the concept of 'act of war' in terms of a 'threat or use of force,' as that phrase is used in the United Nations (UN) Charter. Article 2(4) of the UN Charter provides: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.' ").

(i.e., a kinetic, rather than cyber-based, response).[237] According to one military official, the basic concept is "[i]f you shut down our power grid, maybe we will put a missile down one of your smokestacks."[238] In its 2011 report to Congress announcing its decision, DoD stated:

> [T]he President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interest from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government, or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by DoD.[239]

Notwithstanding DoD's report, defense officials continue to struggle to define exactly what kind of cyberattack constitutes a "use of force" (the equivalent of an armed attack), with some officials of the opinion that the test should be whether or not a cyberattack has an effect equivalent to a conventional attack.[240] Others argue that what is important is the amount of "actual or attempted" damage caused by the attack.[241]

Some early examples of "cyberattacks" include: (1) "Web War I,"[242] in which Russia initiated a barrage of distributed denial of service ("DDoS") attacks on Estonia's "essential electronic infrastructure" in 2007 in response to Estonia's then-controversial decision to relocate a Soviet-era memorial to fallen WWII soldiers;[243] and (2) coordinated Russian cyberattacks on Georgia's Internet infrastructure in connection with the brief war between Russia and Georgia in 2008.[244] Cyberattacks also have

---

237. *Id.* at 4; *see* Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J. (May 30, 2011, 10:30 PM), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html (discussing Pentagon thinking on the issue of what kinds of cyberattacks would be considered a "use of force" potentially triggering retaliation); *id.* ("One idea gaining momentum at the Pentagon is the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a 'use of force' consideration, which could merit retaliation.").

238. *Id.*

239. U.S. DEP'T OF DEF., *supra* note 23, at 4.

240. Gorman & Barnes, *supra* note 237.

241. *Id.*

242. *War in the Fifth Domain*, *supra* note 182.

243. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all ("All major commercial banks, telcos, media outlets, and name servers—the phone books of the Internet—felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation.").

244. David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS J. 1, 2–5 (Jan. 6, 2011), http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

been reported more recently in the ongoing conflicts between North and South Korea,[245] and Israel and Hamas.[246] In contrast, the United States reportedly declined to engage in offensive cyberattacks during the U.S.-led strikes on Libya in March 2011.[247]

High-profile "cyberattacks" emanating from, directed at, or intended to influence the United States reportedly include: (1) Stuxnet; (2) Wiper; (3) Shamoon; and (4) the summer 2012 denial of service attacks on U.S. financial institutions. Each is described in more detail below.

First, the Stuxnet virus reportedly was unleashed as part of a U.S.-Israeli operation to destroy centrifuges at Iran's Natanz nuclear enrichment complex.[248] The operation reportedly began under President George W. Bush and was intended to sabotage Iran's nuclear program.[249] Discovered in June 2010, Stuxnet was "the first attack of a major nature in which a cyberattack was used to effect physical destruction."[250]

Second, like Stuxnet, the Wiper virus reportedly was created by the United States and Israel and was used to systematically delete data and system files from computers as part of an April 2012 cyberattack on Iran's Oil Ministry and affiliates, including the National Iranian Oil Company.[251]

(explaining that Russia used cyber operations to disrupt the Georgian government's ability to communicate strategically with the international community); Robert Haddick, *This Week At War: Lessons From Cyberwar I*, FOREIGN POL'Y (Jan. 28, 2011), http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i ("When the kinetic battle broke out on Aug. 7, Russian government and irregular forces conducted distributed denial-of-service attacks on Georgian government and military sites. These attacks disrupted the transmission of information between military units and between offices in the Georgian government. Russian cyberforces attacked civilian sites near the action of kinetic operations with the goal of creating panic in the civilian population. Russian forces also attacked Georgian hacker forums in order to pre-empt a retaliatory response against Russian targets.").

245. Pierluigi Paganini, *Concerns Mount over North Korean Cyber Warfare Capabilities*, INFOSEC ISLAND (June 11, 2012), http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html.

246. Gwen Ackerman & Saud Abu Ramadan, *Israel Wages Cyberwar with Hamas as Civilians Take up Computers*, BLOOMBERG (Nov. 19, 2012, 5:08 PM), http://www.bloomberg.com/news/2012-11-19/israel-wages-cyber-war-with-hamas-as-civilians-take-up-computers.html.

247. Eric Schimtt & Tom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, N.Y. TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html. American officials "rejected cyberwarfare" out of (1) concern that it might "set a precedent for other nations . . . to carry out such offensives"; (2) concern about mounting the attack "on such short notice"; and (3) inability "to resolve whether the president had the power to proceed with such an attack without informing Congress." *Id.*

248. Sanger, *supra* note 223.

249. *Id.*

250. *Id.*

251. Kim Zetter, *Qatari Gas Company Hit with Virus in Wave of Attacks on Energy*

As one Iranian official explained, "The aim [of Wiper] is to increase pressure so that Iran will compromise in the upcoming nuclear talks on May 23[, 2012]."[252]

Dubbed a "Wiper copycat,"[253] the Shamoon virus was discovered August 16, 2012, after attacking 30,000 computers at Saudi Arabia's state-owned oil company (Aramco) and replacing critical files on those computers with images of a burning American flag. Although the United States has not officially blamed Iran for the attack, it is widely believed that Iran launched the attack in retaliation for Stuxnet. Iran likely targeted Aramco because the company supplied oil to customers who were unable to get oil from Iran after U.S.-led financial sanctions cut Iran's oil exports nearly in half.[254] Just weeks after the Aramco attack, Shamoon attacked computers at Qatar's RasGas, one of the world's largest exporters of liquefied natural gas.[255]

Iran also is believed to be behind the prolonged denial of service attacks against major U.S. financial institutions launched in September 2012, including Bank of America, Wells Fargo, PNC, and others.[256]

If media reports are any indication, concerns over cyberwar appear to have intensified throughout 2012 at the highest levels of the U.S. government, with dire warnings repeatedly emanating from top U.S. defense officials. DHS Secretary Janet Napolitano warned in November 2011 that a cyberattack on critical infrastructure could cause "loss of life" and "huge economic loss."[257] The following summer, six elite U.S.

Companies, WIRED (Aug. 30, 2012, 5:04 PM), http://www.wired.com/threatlevel/2012/08/hack-attack-strikes-rasgas/.

252. Thomas Erdbrink, *Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals from Internet*, N.Y. TIMES (Apr. 23, 2012), http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html.

253. Elinor Mills, *A Who's Who of Mid-East Targeted Malware*, CNET (Aug. 31, 2012, 4:00 AM), http://news.cnet.com/8301-1009_3-57503949-83/a-whos-who-of-mideast-targeted-malware/; Erdbrink, *supra* note 252.

254. Siobhan Gorman & Julian A. Barnes, *Iran Blamed for Cyberattacks: U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy*, WALL ST. J. (Oct. 12, 2012, 7:38 PM), http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html; *see* Nicole Perlroth, *Connecting the Dots After Cyberattack on Saudi Aramco*, N.Y. TIMES BITS BLOG (Aug. 27, 2012, 7:20 PM), http://bits.blogs.nytimes.com/2012/08/27/connecting-the-dots-after-cyberattack-on-saudi-aramco/.

255. Zetter, *supra* note 251.

256. *See* Nicole Perlroth, *Attacks on 6 Banks Frustrate Customers*, N.Y. TIMES (Sept. 30, 2012), http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html; Chris Strohm & Eric Engleman, *Cyber Attacks on U.S. Banks Expose Vulnerabilities*, BUSINESSWEEK (Sept. 28, 2012), http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability.

257. Jason Ryan, *Loss of Life in Major Computer Attack, Warns Homeland Security*,

national security officials[258] urged Congress to pass cybersecurity legislation to protect critical infrastructure, writing:

> We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when 'cyber 9/11' hits—it is not a question of 'whether' this will happen; it is a question of 'when.'[259]

In the fall of 2012, then-Defense Secretary Leon Panetta warned that the U.S. is at risk for a "cyber-Pearl Harbor[;] . . . an attack that would cause physical destruction and the loss of life . . . and create a profound new sense of vulnerability."[260] Panetta said:

> A cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation . . . . The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks.[261]

Finally, in an op-ed published in the *New York Times* on December 6, 2012 to coincide with the anniversary of Pearl Harbor, Senators Lieberman and Collins warned:

> A storm is surely gathering again, and we must resist the false sense of calm. The attack is not a matter of if, but when. It will not be launched

---

ABC NEWS (Oct. 27, 2011, 6:33 PM), http://www.homelandsecuritynewswire.com/dr20111201-congressional-approval-of-cybersecurity-bill-looks-promising.

258. Namely, Michael Chertoff, former Secretary of the Department of Homeland Security; Mike McConnell, former Director of the NSA and former Director of National Intelligence; Paul Wolfowitz, former Deputy Secretary of Defense; Michael Hayden, retired U.S. Air Force four-star general and former Director of both the NSA and the CIA; James Cartwright, retired U.S. Marine Corps four-star general and former Vice Chairman of the Joint Chiefs of Staff; and William Lynn III, a former Deputy Secretary of Defense. Letter from Michael Chertoff et al. to Harry Reid & Mitch McConnell, *supra* note 182.

259. *Id.*

260. Bumiller & Shanker, *supra* note 107. Testifying before the Senate Armed Services Committee in June, 2011, then-Secretary of Defense Leon Panetta said, "The next Pearl Harbor we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems." *Hearing to Consider the Nomination of Hon. Leon E. Panetta to Be Secretary of Defense Before the S. Comm. on Armed Services*, 112th Cong. 25 (June 9, 2011) [hereinafter *Panetta Confirmation Hearing*] (statement of Leon Panetta), http://www.armed-services.senate.gov/Transcripts/2011/06%20June/11-47%20-%206-9-11.pdf.

261. Panetta, *supra* note 223.

> from aircraft carriers, missile silos or massed armies. It will come through cyberspace and will strike our most vital computer systems, those that manage our electricity grids, oil and gas pipelines, telecommunications networks and financial markets. We know that our digital networks are being tested, on a minute by minute basis, by would-be cyberterrorists, criminal gangs, rogue hackers and rival nations who look for unguarded digital back doors that would allow them to seize control of our most essential computers.[262]

Some experts have suggested that cyberwar concerns have been greatly exaggerated. For example, a recent Dartmouth study of cyberwar funded by DHS concluded that "the degree of damage that could be caused in a cyberattack bears no resemblance to an electronic 'Pearl Harbor,' " although "inflicting significant economic costs on the public and private sectors and impairing performance of key infrastructures (via IT networks linked to embedded computer systems, for example) seem both plausible and realistic."[263] Prominent cybersecurity expert James Lewis at the Center for Strategic and International Studies ("CSIS") has repeatedly expressed skepticism of the view that cyberattacks are likely to cause widespread death, damage, and destruction. In a 2003 interview, he said:

> [N]o sane person argues—that a cyber attack could lead to mass casualties. It's not in any way comparable to weapons of mass destruction. In fact, what a lot of people call them is 'weapons of mass annoyance.'[264] If your power goes out for a couple hours, if somebody draws a mustache on Attorney General Ashcroft's face on his Web site, it's annoying. It's irritating. But it's not a weapon of mass destruction. The same is true for this.[265]

---

262. Joseph I. Lieberman & Susan Collins, *At Dawn We Sleep*, N.Y. TIMES (Dec. 6, 2012), http://www.nytimes.com/2012/12/07/opinion/will-congress-act-to-protect-against-a-catastrophic-cyberattack.html.

263. BILLO & CHANG, *supra* note 23, at 7. "Some experts maintain that cyberattacks with potential strategic national security effects, often referred to as an 'electronic Pearl Harbor,' are impossible. Others proclaim they are inevitable." *Id.* at 12.

264. The phrase "weapons of mass annoyance" was coined by Stewart Baker. JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, ASSESSING THE RISKS OF CYBER TERRORISM, CYBER WAR, AND OTHER CYBER THREATS, 11 n.2 (2002), http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

265. *Frontline: Cyberwar!: Interview of James A. Lewis*, (PBS television broadcast Feb. 18, 2003), *available at* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html; *see* LEWIS, *supra*, note 264, at 11 ("Terrorists or foreign militaries may well launch cyber attacks, but they are likely to be disappointed in the effect. Nations are more robust than the early analysts of cyber-terrorism and cyber-warfare give them credit for, and cyber attacks are less damaging than physical attacks. Digital Pearl Harbors are unlikely. Infrastructure systems, because they have to deal with failure on a routine basis, are also more flexible and responsive in restoring

Writing in a similar spirit in 2010, Lewis explained: "[c]yberattacks are not very destructive, compared to other weapons, particularly strategic weapons. It seems fair to say that at this time, the possibility of damage, death and destruction from cyber attack is low. Cyber weapons will have difficulty produc[ing] casualties."[266]

The broad spectrum of expressed views as to the severity of the cyberthreat may be indicative of both the reality and unpredictability of the threat. As Chairman of the Joint Chiefs of Staff General Martin Dempsey stated in 2012, "Cyber is the black swan[267] because we don't know exactly what capabilities exist out there . . . . If you're asking me which of the unknown threats worry me the most—cyber . . . . Cyber is the threat that concerns me the most."[268]

While acknowledging the gravity of the cyber threat, intelligence officials dramatically toned down their cyberwar rhetoric in early 2013. For example, while Director of National Intelligence ("DNI") James Clapper told Congress in March 2013 that cyberattacks are the most dangerous threat facing the United States, he also said that the intelligence community sees only a "remote chance" of a major computer attack on the United States in the next two years.[269]

Rhetoric aside, experts are struggling to identify appropriate responses to nation-state cyberattacks.[270] The administration took a small step forward with respect to one aspect of these difficult issues in mid-October, when President Obama reportedly signed Presidential Decision Directive 20 ("PDD-20").[271] Although classified, PDD-20 guides federal agency

---

service than early analysts realized. Cyber attacks, unless accompanied by a simultaneous physical attack that achieves physical damage, are short lived and ineffective. However, if the risks of cyber-terrorism and cyber-war are overstated, the risk of espionage and cyber crime may be not be fully appreciated by many observers.").

266. LEWIS, *supra* note 264, at 3.

267. *Black Swan Definition*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/english/black%2Bswan (last visited Apr. 1, 2013) (defining "black swan" as "an unpredictable or unforeseen event, typically one with extreme consequences . . . .").

268. ForaTv, *Martin Dempsey: Cyber Attacks are Black Swan Threat to US*, YOUTUBE (Aug. 22, 2012), http://www.youtube.com/watch?v=aDAG1dJNu4Q.

269. Mazzetti & Sanger, *supra* note 223 (describing a "major" attack as one resulting in "long-term, wide-scale disruption of services, such as a regional power outage").

270. Jonathan Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV., no. 3, 2010, at ¶ 1 ("Cyber attacks do not fit neatly into the traditional international framework governing the use of force.").

271. Ellen Nakashima, *Obama Signs Secret Directive to Help Thwart Cyberattacks*, WASH. POST (Nov. 14, 2012), http://www.washingtonpost.com/world/national-

responses to cyberthreats and "attempts to settle years of debate among government agencies about who is authorized to take what sorts of actions in cyberspace and with what level of permission."[272] PDD-20 reportedly is "the most extensive White House effort to date to wrestle with what constitutes an 'offensive' and a 'defensive' action in the rapidly evolving world of cyberwar and cyberterrorism."[273]

As experts debate the proper definition and response to nation-state cyberattacks,[274] another great challenge looms: understanding how we, as a nation, should address the threat of state actors engaging in highly disruptive (and potentially economically destabilizing) activities in the .com domain—e.g., electronically manipulating the stock market or triggering communications outages—that are not accompanied by the loss of life or physical destruction typically associated with acts of war. While some support giving U.S. Cyber Command the flexibility to defend critical infrastructures against cyberthreats, others have deep concerns about allowing the military to operate outside of the .mil context, including concerns that military cyberoperations could lead to unintentional collateral damage, such as shutting down a hospital generator.

Finally, compounding the cyberwar threat is an increasingly sophisticated, and entirely unregulated, market for so-called "zero-day" exploits.[275] Zero-day exploits are previously unknown cyber-vulnerabilities that can be used in a cyberattack.[276] Some liken zero-day exploits to cyberweapons[277] because they essentially "provide keys to the doors through which cyberwarfare can be waged."[278] Hackers and others who discover such exploits can make their findings public, work with vendors to fix the security flaws, use the exploits for their own purposes, or sell the exploits to security firms, black-marketers, or nation-states. Some hackers have even suggested that corporate IT departments could become profit centers by developing offensive exploits and selling them to the United States and allied governments.[279] Nation-states may purchase

---

security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

272. *Id.* (describing contents of PDD-20).

273. *Id.*

274. *See* Ophardt, *supra* note 270, at ¶ 1.

275. *See generally* Greenberg, *supra* note 146 (documenting the black market for so-called "zero-day" exploits or "cyberweaponry").

276. *Id.*

277. *Id.* (quoting privacy activist Chris Soghoian that "zero-day" exploits are the "bullets for cyberwar").

278. Ophardt, *supra* note 270, at ¶ 18.

279. Jeffrey Carr, *Flipping Malware: A Profit Opportunity for Corporate IT Departments*, INFOSEC ISLAND (Dec. 9, 2012), http://www.infosecisland.com

exploits with the "explicit intention of invading or disrupting the computers and phones of crime suspects and intelligence targets."[280] Accordingly, some hackers reportedly "self-regulate," limiting the foreign interests to whom they are willing to sell or refusing to sell to foreign interests at all.[281]

V. RECENT CONGRESSIONAL AND EXECUTIVE ACTION

One of the most fundamental cybersecurity issues facing our nation is the appropriate role of government in helping the private sector—which owns and operates approximately 85% of the United States' critical infrastructure[282]—address cybersecurity risks to its operations. Although the U.S. has long relied primarily on a market-based approach to cybersecurity, a host of laws and regulations, some of which were passed over a decade ago, have effectively forced cybersecurity investment in certain industry sectors, most notably the financial and health sectors.[283]

/blogview/22777-Flipping-Malware-A-Profit-Opportunity-for-Corporate-IT-Departments.html.

280. Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)*, FORBES (Mar. 21, 2012, 9:08 AM), http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/.

281. *Id.* (reporting that vulnerability research company, Vupen, claims that it carefully screens its clients, selling only to NATO governments and "NATO partners," but that Vupen admits that there is no way to ensure that clients will not sell its products to another entity).

282. *See* TELECOMMS. INDUS. ASS'N, SECURING THE NETWORK: CYBERSECURITY RECOMMENDATIONS FOR CRITICAL INFRASTRUCTURE AND THE GLOBAL SUPPLY CHAIN 1 (2012), http://tiaonline.org/sites/default/files/pages/TIACybersecurityWhitePaper_0.pdf (estimating that approximately eighty to ninety percent of the nation's critical infrastructure is privately-owned); *see also* SPADE, *supra* note 23, at 25 ("[Privately-owned telecommunications companies] own and operate most of America's cyber infrastructure—that is, the cables, servers, routers, and switches that connect cyberspace. The same is true for the Supervisory Control and Data Acquisition ("SCADA") systems that run America's physical infrastructure: power, water, and communications. SCADA control functions are intranets, but are usually connected to the global Internet.").

283. *See, e.g.*, Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108–159, 117 Stat. 1952 (2003) (codified as amended in scattered Sections of 15 and 20 U.S.C.) ("FACTA"); Gramm-Leach-Bliley Financial Services Modernization Act of 1999, §§ 501–527, 15 U.S.C. §§ 6801–27 ("GLB"); Health Insurance Portability and Accountability Act of 1996, Pub. L. N. 104–191, 110 Stat. 1936 (1996) (codified as amended in scattered Sections of 18, 26, 29 and 42 U.S.C.) ("HIPAA"); FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.1–14.5 (2012) (implementing "safeguards" provisions of Gramm-Leach-Bliley); Protection of Digital Computer and Communication Systems and Networks, 10 C.F.R. § 73.54 (2012); Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718 (Nov. 9, 2007); *see also* MARK E. SCHREIBER ET AL., EDWARDS WILDMAN PALMER LLP, EVERYONE'S NIGHTMARE: PRIVACY AND DATA BREACH RISKS 25–44 (2012), http://www.acc.com/chapters/ne/loader.cfm?csModule=security/getfile&PageID=1300198 (discussing data security laws and regulations);

More recently, Congress and federal regulators have adopted a number of legislative and regulatory measures to improve transparency with respect to cyberincidents.[284] The measures most obviously designed to improve transparency are data breach notification laws. Pursuant to these laws, corporations must, under certain circumstances, disclose data breaches. As of August 2012, forty-six states[285] and the federal government[286] had

---

Stewart Baker & Melanie Schneck-Teplinsky, *Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US, in* CYBERCRIMES: A MULTIDISCIPLINARY ANALYSIS 243–48 (Sumit Ghosh & Elliot Turrini eds., 2010) (discussing financial and medical data security laws and regulations, including GLB, HIPAA, Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act"), and FACTA).

284. Such efforts are not limited to the United States. The provisions of the European Commission's draft data protection regulation now under consideration in the European Union require data controllers to "notify data breaches" and impose administrative sanctions for failure to do so. *See Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Process of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, arts. 31–32, at 11, art. 79, at 15 COM (2012) 11 final (Jan. 25, 2012), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri =COM:2012:0011:FIN:EN:PDF. Articles 31 and 32 require companies to notify their supervisory authority and affected individuals within 24 hours of discovery of a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." Article 79 provides that:

> The supervisory authority shall impose a fine up to 1,000,000 EUR or, in case of an enterprise up to 2% of its annual worldwide turnover, to anyone who, intentionally or negligently . . . does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32.

Id.

285. Every state has passed a data breach notification law except Alabama, Kentucky, New Mexico, and South Dakota. *See State Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated Aug. 20, 2012) (indicating that 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted security breach notification laws); *see also State Data Breach Notification Laws*, MINTZ LEVIN, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/statedatabreachmatrix.pdf (last updated Dec. 1, 2012) (providing a downloadable matrix of state data breach laws current as of December 2011).

286. The federal data breach notification law, codified at 42 U.S.C. § 17932, is one of several amendments to HIPAA set forth in the privacy provisions of the Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. §§ 17921, 17931–40, 17951–53 (2009). The HITECH Act was embedded into the stimulus bill that President Obama signed into law on February 17, 2009. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (codified as amended in scattered Sections of 6, 19, 26, and 42 U.S.C.). The HITECH

adopted such laws. SEC disclosure rules also serve to improve transparency. Specifically, the SEC Division of Corporation Finance issued staff-level guidance on October 13, 2011, at Senator John D. Rockefeller's (D-W.Va.) urging,[287] that requires companies report to the SEC "material information regarding cybersecurity risks and cyber incidents."[288] Appropriate disclosures may include, among other things, "[A d]escription of cyberincidents experienced by the [SEC] registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences . . . ."[289] Senator Rockefeller has since urged

---

Act effectively provides a safe-harbor from its breach notification requirements when protected health information ("PHI") is "secured" (e.g., encrypted using NIST-approved processes), giving covered entities and their business associates a strong incentive to maintain electronic PHI in NIST-approved encrypted form at all times. In the summer of 2009, the Department of Health and Human Services ("HHS") published an interim final "Breach Notification Rule" implementing HITECH's breach reporting requirements. *See* Breach Notification for Unsecured Protected Health Information, Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009), http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf (requiring covered entities under the HIPAA and their business associates to provide notification in the case of breaches of unsecured protected health information). *Breach Notification Final Rule Update*, U.S. DEP'T OF HEALTH AND HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html (last visited Apr. 1, 2013). The FTC issued companion breach notification regulations, FTC Health Breach Notification Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009). On January 25, 2013, HHS issued a final rule that, *inter alia*, modified the Breach Notification Rule. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566–5702 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164). Among other things, the final rule amended the definition of "breach" used in the regulations so as to "replace[] the [B]reach [N]otification [R]ule's 'harm' threshold with a more objective standard." 78 Fed. Reg. 5566, 5695. Specifically, breach notification was not required under the interim rule if a covered entity or business associate could "demonstrate that there [was] no significant risk of harm to the individual," 78 Fed. Reg. 5641, but under the final rule, a breach is presumed unless "the covered entity or business associate . . . demonstrates [through a risk assessment] that there is a low probability that the protected health information has been compromised." 78 Fed. Reg. 5695.

287. Elizabeth Wasserman, *SEC Urged to Give Stronger Guidance on Cyber Disclosure*, BLOOMBERG (Apr. 10, 2013, 9:57 AM), http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html ("Rockefeller in May 2011 wrote to then-SEC Chairman Mary Schapiro pointing out the growing risk posed to U.S. companies by 'malicious actors' who 'attack and disrupt computer networks to steal valuable trade secrets, intellectual property, and financial and confidential information.' He asked the SEC to develop and publish guidance to clarify disclosure requirements pertaining to 'information security risk, including material information security breaches involving intellectual property or trade secrets.' ")

288. *CF Disclosure Guidance: Topic No. 2*, SEC (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

289. *Id.*

the SEC to adopt formal cybersecurity guidance. In an April 10, 2013 letter to incoming SEC Chairman, Mary Jo White, Senator Rockefeller wrote:

> While the [SEC] staff guidance has had a positive impact on the information available to investors on these matters, the disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices . . . . Investors deserve to know whether companies are effectively addressing their cybersecurity risks—just as investors should know whether companies are managing their financial and operational risks . . . . Formal guidance from the SEC on this issue will be a strong signal to the market that companies need to take their cybersecurity efforts seriously.[290]

Laws, regulations, and guidance on data breach notification arguably help the market function more efficiently by enabling it to evaluate companies in part based on their ability to keep their networks secure. The more information is available about cyberincidents and cyberthreats, the better the cybersecurity market should function, since more reliable data will help corporations more accurately calculate efficient levels of cybersecurity. Accordingly, disclosure-forcing rules are often viewed as part of a larger effort to combat what some believe to be chronic U.S. private sector underinvestment in cybersecurity.

Vulnerability mitigation has long been the cornerstone of U.S. cybersecurity policy,[291] with legislators struggling to properly incentivize corporations to improve their cyberdefenses without dampening

290. Elizabeth Wasserman, *SEC Urged to Give Stronger Guidance on Cyber Disclosure*, BLOOMBERG, (Apr. 10, 2013, 9:57 AM), http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html.http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e.

291. *See, e.g.*, WHITE HOUSE, CYBERSPACE POLICY REVIEW, *supra* note 2, at i, iii ("It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution. . . . Without major advances in the security of [the nation's digital infrastructure] systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations."); *see also* Hathaway, *supra* note 156, at 78 ("[R]eal [cybersecurity] leadership requires adopting and embedding sometimes-costly security solutions into our core infrastructures and enterprises . . . ."); Press Release, Mac Thornberry, U.S. Representative, Thornberry Named Leader of New Cybersecurity Task Force (June 24, 2011), *available at* http://thornberry.house.gov/news/documentsingle.aspx?DocumentID=248853 (quoting House Majority Leader Eric Cantor (R-Va.) as saying that " '[s]trengthening our networks' security is fundamental to protecting our national and financial security, promoting economic growth, and creating jobs").

innovation.[292] The 2012 congressional session was no exception, as Senators vigorously debated the merits of legislation that would have set minimum cybersecurity standards for the private sector. Also at issue in that session was legislation designed to facilitate the flow of information—in both directions—between the private sector and the U.S. government.

A. Congressional Action (2011–2012)

A flurry of cybersecurity-related activity in both houses of Congress during the 112th Congress ultimately led to successful passage of a controversial cybersecurity bill in the House in April of 2012, but failure to pass cybersecurity legislation in the Senate during the 2012 session. Despite Congress' failure to pass cybersecurity legislation, the debate over the bills that were considered is described in some detail below as it informs current discussions about the appropriate way forward.

1. Administration Legislative Proposal

On May 12, 2011, the Administration submitted cybersecurity legislation to Congress.[293] At the core of the seven-part package were provisions giving DHS authority to regulate critical infrastructure.[294] These provisions required owners and operators of critical infrastructure to develop cybersecurity plans, the implementation of which was to be evaluated by the Secretary of DHS.[295]

2. U.S. House of Representatives

a. Republican Cybersecurity Task Force

In June of 2011, House Republicans announced the creation of a GOP-

292. There have been approximately thirty cybersecurity proposals in the House and Senate since 2009. *See* David Perera, *Congressional Cybersecurity Bill Roundup*, FIERCEGOVERNMENTIT (May 12, 2010), http://www.fiercegovernmentit.com/story/congressional-cybersecurity-bill-roundup/2010-05-12 (listing cybersecurity bills introduced during 111th Congress, i.e., January 3, 2009 through January 3, 2011); *see also* ERIC A. FISCHER, CONG. RESEARCH SERV., R 42114, FEDERAL LAWS RELATING TO CYBERSECURITY: DISCUSSION OF PROPOSED REVISIONS 4–8 (2012), http://www.fas.org/sgp/crs/natsec/R42114.pdf (discussing selected cybersecurity legislative proposals considered in the 112th Congress).

293. EXEC. OFFICE OF THE PRESIDENT, OFFICE OF MGMT. & BUDGET, LAW ENFORCEMENT PROVISIONS RELATED TO COMPUTER SECURITY (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

294. *See generally* EXEC. OFFICE OF THE PRESIDENT, OFFICE OF MGMT. & BUDGET, CYBERSECURITY REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE ACT (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act.pdf.

295. *Id.* §§ 5–6.

only task force to study cybersecurity and make recommendations to House leadership.[296] The resulting task force report, issued in October of 2011, departed from the Administration's proposal in several important respects.[297] Most notably, the task force unanimously recommended adoption of voluntary cybersecurity standards tied to incentives to improve cybersecurity.[298] Representative Thornberry (R-TX), leader of the task force, subsequently explained that incentives help to "elevate [cybersecurity] in the consciousness of CEOs and businesses."[299] The task force specifically recommended that Congress consider research and development tax credits for cyberinvestments and consider whether cybersecurity insurance can help improve security.[300] The task force also recommended that Congress use federal purchasing power to improve cybersecurity by revising the Federal Acquisition Regulations to require appropriate security in all federal IT procurements.[301] At the event announcing completion of the task force report, Thornberry declared: "anybody who gets a federal grant ought to have some sort of minimum level of cybersecurity."[302] Despite differences between the Administration's legislative proposal and the task force recommendations, in December 2011, Senate Majority Leader Harry Reid (D-NV) described the House Republican cybersecurity task force recommendations as "fully consistent with our efforts."[303]

---

296. Press Release, Rep. Mac Thornberry, *supra* note 291.

297. *See, e.g.*, MAC THORNBERRY ET AL., RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE 7–8 (2011), http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf. The task force *agreed* with the White House on "the need to simplify data-breach reporting requirements for companies, update information-security standards for government agencies, and boost recruitment of qualified cybersecurity workers." Eric Engleman, *House Republican Cybersecurity Plan Echoes Part of Obama Policy*, BLOOMBERG (Oct. 6, 2011, 12:01 AM), http://www.bloomberg.com/news/2011-10-05/house-cybersecurity-task-force-wary-of-rules-on-network-defense.html.

298. THORNBERRY ET AL., *supra* note 297, at 7–8; Engleman, *supra* note 297 (explaining that the report also recommended that Congress facilitate the creation of a non-government clearinghouse for information-sharing among businesses and the government). Task force leader Rep. Thornberry also noted that about fifty outdated laws related to cybersecurity need to be revised and he noted that "basic hygiene" steps could eliminate the majority of malware. *Id.*

299. Zach Rausnitz, *House Cybersecurity Task Force Suggest Incentives, Info-Sharing*, FIERCE HOMELAND SEC. (Oct. 12, 2011), http://www.fiercehomelandsecurity.com/story/house-cybersecurity-task-force-suggests-incentives-info-sharing/2011-10-12#ixzz2EnMEIhif.

300. THORNBERRY ET AL., *supra* note 297, at 8.

301. *See id.* at 19.

302. Rausnitz, *supra* note 299.

303. Gautham Nagesh, *Reid says Senate will take up cybersecurity bill next year*, THE HILL (Nov. 17, 2011, 11:52 AM), 194245-senate-will-take-up-cybersecurity-bill-

b. CISPA

Ultimately, the House did not pass legislation based on the recommendations of its cybersecurity task force. Instead, on April 26, 2012, after nearly seven hours of debate,[304] the U.S. House of Representatives passed the Cyber Intelligence Sharing and Protection Act ("CISPA") of 2012,[305] a highly controversial bill that, according to legislative sponsors, was designed to address the Chinese and Russian cyberespionage threat[306] and protect critical infrastructure.[307]

The purpose of CISPA was to remove legal obstacles to information sharing[308] between private sector companies and the U.S. government in two ways. First, CISPA was drafted to give the intelligence community the authority to share cyber threat intelligence, including classified intelligence, with certain private-sector entities under certain conditions.[309]

---

next-year.

304. Declan McCullagh, *How CISPA Would Affect You (faq)*, CNET (Apr. 27, 2012, 4:00 AM), http://news.cnet.com/8301-31921_3-57422693-281/how-cispa-would-affect-you-faq/.

305. H.R. 3523, 112th Cong. (2012). CISPA is also known as the Rogers-Ruppersberger bill after Mike Rogers (R-Mich.) and Dutch Ruppersberger (D-Md.), the chairman and the ranking member of the House Permanent Select Committee on Intelligence ("HPSCI"), respectively.

306. *See* Declan McCullagh, *House Passes CISPA Internet Surveillance Bill*, ZDNET (Apr. 27, 2012, 5:00 AM), http://www.zdnet.com/news/house-passes-cispa-internet-surveillance-bill/6360341 ("[HPSCI Chairman Rogers said that CISPA is] needed to stop the Chinese government from stealing our stuff [and that the Chinese are] stealing the value and prosperity of America."); Press Release, Rep. Mike Rogers, Co-Sponsors Top 100 for the Rogers-Ruppersberger Bipartisan Cyber Bill (Mar. 29, 2012), *available at* http://mikerogers.house.gov/news/documentsingle.aspx?DocumentID=287920 ("Every day U.S. businesses are targeted by nation-state actors like China for cyber exploitation and theft . . . . This consistent and extensive cyber looting results in huge losses of valuable intellectual property, sensitive information, and American jobs. The broad base of support for this bill shows that Congress recognizes the urgent need to help our private sector better defend itself from these insidious attacks . . . .").

307. Press Release, Rep. Mike Rogers, *supra* note 306 (quoting HPSCI Ranking Member C.A. Dutch Ruppersberger) ("Without important, immediate changes to American cybersecurity policy, I believe our country will continue to be at risk for a catastrophic attack to our nation's vital networks—networks that power our homes, provide our clean water or maintain the other critical services we use every day. This small but important piece of legislation is a decisive first step to tackle the cyber threats we face.").

308. James A. Lewis, *Code Red*, FOREIGN POL'Y (Aug. 1, 2012), http://www.foreignpolicy.com/articles/2012/08/01/code_red ("[Information to be shared] can include 'signatures' and other cyberthreat indicators, such as intelligence information, reports of successful penetrations, and information on the identities or network addresses of the 'attacking computers . . . .' ").

309. *See* H.R. 3523 § 1104(a)(1) (amending the National Security Act of 1947 to require the Director of National Intelligence "to establish procedures to allow elements of the intelligence community to share cyber threat intelligence [including classified

Second, CISPA was designed to encourage businesses to voluntarily share cyberthreat information with the government by offering a variety of protections, including exemptions from liability;[310] limitations on government disclosure of shared information, including a Freedom of Information Act ("FOIA") exemption;[311] and prohibition on government use of shared cyberthreat information for regulatory purposes.[312]

Supporters of CISPA describe it as an "information sharing" bill. They say it "helps the private sector defend itself from advanced cyber threats, without imposing any new federal regulations or unfunded private sector mandates, and contains protections for privacy and civil liberties."[313] Opponents include not only an array of privacy and civil liberties advocates, who claim that CISPA will make it easier for the federal government to access personal information,[314] but also those who see the

---

intelligence] with private-sector entities"); *id.* § 1104(a)(2)(A) (classified cyber threat intelligence may only be shared with "certified entities" or persons with "an appropriate security clearance"); *id.* § 1104(a)(2)(C) ("[C]lassified cyber threat intelligence may only be . . . used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure."); *id.* §1104(a)(3)(B) (providing authority to "grant a security clearance on a temporary or permanent basis to a certified entity" and grant "approval to use appropriate facilities"). Taken together, these provisions allow the government to share classified threat information with businesses under certain specific conditions. For example, businesses receiving classified threat information may need security clearances for personnel and technical, administrative, and procedural safeguards to handle classified information.

310. *Id.* § 1104(b)(4)(A) ("No civil or criminal cause of action shall lie or be maintained in Federal or State court against a [cybersecurity provider or certain other designated entities] acting in good faith for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section . . . .").

311. *Id.* § 1104(b)(3)(C)(i) (providing that cyberthreat information shared with the federal government "shall be exempt from disclosure under section 552 of title 5, United States Code [i.e., FOIA]"); *id.* §1104(b)(3)(C)(ii) (providing that cyberthreat information shared with the federal government "shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information").

312. *Id.* §1104(b)(3)(C)(iii).

313. Press Release, Rep. Mike Rogers, *supra* note 306.

314. *See* Chloe Albanesius, *Internet Groups Launch Anti-CISPA Protest*, PC MAG. (Apr. 16, 2012, 12:28 PM), http://www.pcmag.com/article2/0,2817,2403080,00.asp; *see also* Declan McCullagh, *Advocacy Group Flip-Flops Twice Over CISPA Surveillance Bill*, CNET (Apr. 25, 2012, 10:53 PM), http://news.cnet.com/8301-31921_3-57421624-281/advocacy-group-flip-flops-twice-over-cispa-surveillance-bill/ (discussing positions taken by the Center for Democracy and Technology, the American Civil Liberties Union, and the Electronic Frontier Foundation); Greg Nojeim, Jim Dempsey, & Leslie Harris, *A Recap of Months of CDT Advocacy on CISPA*, CTR. FOR DEMOCRACY & TECH. (Apr. 26, 2012), https://www.cdt.org/blogs/2604recapping-state-play-cispa ("Since CISPA was introduced, CDT has consistently said the bill has three critical civil liberties problems . . . . The first is that CISPA permits unfettered sharing of private communication with

bill as doing little to advance cybersecurity.[315] As one cybersecurity expert bluntly stated: "sharing information is a feeble response to a serious threat."[316] President Obama was equally decisive—although somewhat more reserved—when he weighed in on the issue in a July 2012 op-ed, stating, "Simply sharing more information is not enough. Ultimately, this is about security gaps that have to be filled."[317]

CISPA was an enormously controversial bill.[318] Although the bill's sponsors amended CISPA just days before it passed the House ostensibly to address privacy and civil liberties concerns, several of the most controversial provisions in the bill remained untouched. One such provision is § 1104(b)(1)(B) which provides as follows:

> Notwithstanding any other provision of law, a self-protected entity[319] may, for cybersecurity purposes—
>
> (i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and
>
> (ii) share such cyber threat information with any other entity, including the Federal Government.[320]

CISPA critics maintain that the phrase "notwithstanding any other provision of law" allows the private sector to share threat information with the government regardless of existing federal and state laws—including

---

the government; second, it permits that sharing to go to any agency including the super-secret NSA; and third, it permits the government to use this information for purposes wholly unrelated to cybersecurity. On these grounds we oppose CISPA.").

315. Mac Thornberry, *Cybersecurity Needs Our Full Attention*, POLITICO (Apr. 25, 2012, 9:24 PM), http://www.politico.com/news/stories/0412/75604.html #ixzz2EntrTr5D (supporting CISPA, but noting the most prominent criticism is that CISPA "does not go far enough").

316. Lewis, *supra* note 308.

317. Obama, *supra* note 100.

318. The controversy over CISPA stemmed in part from its substantive provisions and in part from comparisons—some unwarranted—of CISPA to the Stop Online Privacy Act ("SOPA"), H.R. 3261, and PROTECT IP Act ("PIPA"), S.B. 968, legislation that was roundly condemned in the technology community months before. *See* Violet Blue, *Say 'Hello' to CISPA, It Will Remind You of SOPA*, CNET (Apr. 13, 2012, 7:35 AM), http://news.cnet.com/8301-1023_3-57413627-93/say-hello-to-cispa-it-will-remind-you-of-sopa/; Rebecca Greenfield, *Why CISPA is Worse Than SOPA*, THE ATLANTIC WIRE (Apr. 27, 2012), http://www.theatlanticwire.com /technology/2012/04/why-cispa-worse-sopa/51638/; Megha Rajagopalan, *Is CISPA SOPA 2.0? We Explain the Cybersecurity Bill*, PROPUBLICA (Apr. 26, 2012, 11:16 AM), http://www.propublica.org/article/is-cipsa-sopa-20-we-explain-the-cybersecurity-bill.

319. A "self-protected entity" is "an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself." Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. § 1104(h)(12).

320. *Id.* § 1104(b)(1)(B).

laws such as the Electronic Communications Privacy Act[321]—some of which specifically limit such sharing in order to protect information privacy and civil liberties. Moreover, critics maintain that use of such sweeping language could have "unforeseen consequences."[322]

Another highly controversial aspect of CISPA—and one that was not addressed by amendments—was that it permits the private sector to share cyberthreat information directly with the National Security Agency ("NSA").[323] Rhetoric began to fly when this provision was interpreted in some circles as raising the specter of government surveillance. Representative Jared Polis (D-Co) argued: "Allowing the military and NSA to spy on Americans on American soil goes against every principle this country was founded on."[324] HSPCI Chairman Rogers defended CISPA, saying: "There is no government surveillance, none, not any in this bill."[325] In fact, CISPA does not include a formal grant of surveillance authority to NSA, but the bill arguably "usher[s] in a new era of information sharing between companies and government agencies—with limited oversight and privacy safeguards."[326] The Administration took the position that CISPA "effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres."[327]

---

321. 18 U.S.C. §§ 2511–22 (2012).

322. RICHARD S. BETH, CONG. RESEARCH SERV., RS 20617, HOW BILLS AMEND STATUTES 1–2 (2003), http://assets.opencrs.com/rpts/RS20617_20030804.pdf ("[A] bill may preface new provisions being added to law with such a phrase as, 'notwithstanding any other provision of law.' Such a phrase tends to imply that the new language is intended to supersede any conflicting provisions of previous law. This broad phrase, however, does not specify which provisions it is meant to refer to, and may therefore have unforeseen consequences for both existing and future laws.").

323. House leadership did not allow for amendments on this issue. The Center for Democracy and Technology ("CDT"), which had vigorously opposed CISPA, came to an informal understanding with the House Intelligence Committee that, in return for CDT's willingness not to oppose CISPA moving forward, the House would consider amendments on what CDT considered to be two major privacy and civil liberties issues in CISPA—"the flow of internet data directly to the NSA and the use of information for purposes unrelated to cybersecurity . . . ." When the House leadership subsequently blocked amendments on both issues, CDT reasserted its opposition to CISPA. *See* Press Release, Ctr. for Democracy & Tech., CDT Opposes CISPA Going Forward (Apr. 25, 2012), *available at* https://www.cdt.org/prstatement/cdt-opposes-cispa-going-forward.

324. McCullagh, *supra* note 306.

325. Josh Smith, *Bucking Veto Threat, House OKs CISPA Cybersecurity Information-Sharing Bill*, NAT'L J. (Apr. 26, 2012, 7:02 PM), http://www.nationaljournal.com/tech/bucking-veto-threat-house-oks-cispa-cybersecurity-information-sharing-bill-20120426.

326. McCullagh, *supra* note 304.

327. *Id.*

Other controversial provisions of CISPA were amended before its passage. For example, after critics lambasted the bill's original language allowing the government to use information shared under CISPA for "any lawful purpose," the bill was amended to limit government use and retention of shared information to five enumerated purposes: (1) cybersecurity;[328] (2) investigation and prosecution of cybersecurity crimes; (3) protection of individuals from the danger of death or serious bodily harm and investigation and prosecution of crimes involving such dangers; (4) protection of minors from harm and/or exploitation (including sexual exploitation, kidnapping, and trafficking); and (5) protection of U.S. national security.[329] While acknowledging that these changes were a step in the right direction, critics nonetheless expressed concern that the amended language continued to permit "information shared under CISPA [to] be used in criminal proceedings against individuals [even though] it can be collected without any Fourth Amendment considerations."[330]

CISPA supporters were quick to note that the bill does not obligate private sector companies to share information with the government; participation in information sharing is entirely voluntary.[331] But critics contended that "the cost of this information sharing—in terms of privacy lost and civil liberties violated—is borne by individual customers and Internet users. For them, nothing about CISPA is voluntary[,] and for them there is no recourse," because CISPA affords broad liability protection to companies who share information and exempts shared information from FOIA.[332]

The Obama administration threatened to veto CISPA unless it ramped up protections for critical infrastructure and privacy protections,[333] but much

328. The definition of "cybersecurity" was itself limited by the amendments.

329. Cyber Intelligence Sharing and Protection Act, H.R. 3523 112th Cong. § 1104(c)(1) (2012).

330. Alexander Furnas, *Can Last-Minute Amendments Redeem the Troubling Cybersecurity Bill?*, THE ATLANTIC (Apr. 25, 2012, 6:45 PM), http://www.theatlantic.com/technology/archive/2012/04/can-last-minute-amendments-redeem-the-troubling-cybersecurity-bill/256372/. CISPA's definition of "cyber threat intelligence" also was amended to address criticisms of over-breadth, but remains controversial. *See* Anjali Dalal, *Why the Cyber Intelligence Sharing and Protection Act (CISPA) Is Not the Solution to U.S. Cyber Attack Fears*, JUSTIA (May 2, 2012), http://verdict.justia.com/2012/05/02/why-the-cyber-intelligence-sharing-and-protection-act-cispa-is-not-the-solution-to-u-s-cyber-attack-fears (detailing how CISPA may circumvent the Fourth Amendment).

331. David Inserra, *CISPA Is Ready for Primetime*, THE FOUNDRY (Apr. 25, 2012, 6:30 PM), http://blog.heritage.org/2012/04/25/cispa-is-ready-for-prime-time/.

332. Furnas, *supra* note 330.

333. Andrew Couts, *CISPA Cybersecurity Bill Passes House 248 to 168*, DIGITAL TRENDS (Apr. 26, 2012), http://www.digitaltrends.com/web/cispa-cybersecurity-bill-passes-house-248-to-168/#ixzz2DuTt6QBq.

of the technology industry supported CISPA,[334] apparently in hopes that Congress would otherwise remain hands-off with respect to cybersecurity.[335]

One cybersecurity expert summarized the CISPA saga as follows:

> Congress knows that weak cybersecurity endangers the country—and that America is dangerously unprepared—but it cannot muster a majority to support serious defensive measures. The same forces that have kept Capitol Hill in gridlock on many important issues have also blocked effective cybersecurity legislation. That said, Congress does not want to be in the position, after the inevitable cyberdisruption, of having to say it knew but did nothing. The political solution to gridlock is to pass weak legislation and pretend it will work. This is the CISPA story.[336]

3. U.S. Senate

The Senate ultimately failed to pass cybersecurity legislation in 2012, however a number of bills made their way through the Senate, the most important of which were: (1) the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act ("SECURE-IT") of 2012;[337] (2) the Cybersecurity Act of 2012 ("CSA");[338] and (3) the Revised Cybersecurity Act of 2012.

a. SECURE-IT Act

The SECURE-IT Act of 2012, sponsored by Senator McCain and other Republicans, was an information-sharing bill. It enabled private sector "cyberthreat information" sharing with the government, including NSA. The bill was first introduced in February and was re-introduced in June with changes designed to address criticisms of the original bill. According to its sponsors, the Act "recognizes industry's central role in protecting cyber networks and provides it the liability protection it needs to share real-time cyber threat information that is necessary to combat cyber attacks."[339]

---

334. *H.R. 3523 Letters of Support*, H. PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/hr-3523-letters-support (last visited Apr. 1, 2013) (listing numerous letters of support from trade associations such as BSA, Business Roundtable, and the U.S. Chamber of Commerce as well as individual companies such as AT&T, Boeing, Facebook, Lockheed Martin, Microsoft, Oracle, Symantec, and Verizon).

335. Lewis, *supra* note 308 ("One powerful motive for [CISPA's] passage, as a House member privately told companies, was that it would 'help protect you from regulation.' ").

336. *Id.*

337. Introduced as S. 2151 on March 1, 2012; re-introduced as S. 3342 on June 27, 2012.

338. Introduced as S. 2105 on February 14, 2012; re-introduced as S. 3414 on July 19, 2012.

339. Press Release, Senator John McCain, Senators Renew Push to Strengthen

Civil liberties groups were highly critical of both the original and re-introduced bills,[340] asserting, for example, that the legislation's vague definition of "cyberthreat information" could lead to government invasions of personal privacy.[341] More fundamentally, civil libertarians labeled SECURE-IT a "backdoor wiretap bill."[342] They claimed that despite modifications of some of the bill's provisions:

> SECURE IT still allows far too much information to flow to the government, allows information to flow directly from companies in the private sector to the NSA and other elements of the Department of Defense, and allows shared cyber threat information to be used for non-cybersecurity purposes such as national security and law enforcement. Much of this information would otherwise be protected from government access by the Fourth Amendment warrant requirement. Bypassing the warrant requirement to facilitate intelligence and law enforcement investigative activity effectively turns cybersecurity information sharing into a back-door wiretap. The incremental, pro-privacy changes made to SECURE IT [when it was re-introduced in June] do not overcome these fundamental flaws in the legislation.[343]

The SECURE-IT Act stood in stark contrast to the CSA (described in more detail below). SECURE-IT took a market-based, rather than regulatory, approach and gave the federal government no new regulatory authority with respect to cybersecurity standards. In the House, Reps. Mary Bono Mack (R-Cal.) and Marsha Blackburn (R-Tenn.) introduced legislation that mirrors SECURE-IT, with only minor changes.[344]

b. Cybersecurity Act

CSA was originally introduced in February of 2012 by Senators

---

Cybersecurity (June 27, 2012), *available at* http://www.mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=2ed8acb7-cb2a-043e-7bb4-26766aaa2b5b.

340. Greg Nojeim & Jon Miller, *SECURE-IT: Building a Better Back-Door Wiretap*, CTR. FOR DEMOCRACY & TECH. (July 30, 2012), https://www.cdt.org/blogs/greg-nojeim/3007secure-it-building-better-back-door-wiretap (outlining what CDT viewed as "fundamental flaws" in SECURE-IT); Letter from Coalition in Opposition of SECURE-IT to U.S. Senators (May 14, 2012), https://www.cdt.org/files/pdfs/SecureIT_Coalition_Letter.pdf.

341. Nojeim & Miller, *supra* note 340 (outlining what CDT viewed as "fundamental flaws" in SECURE-IT).

342. *Id.*

343. *Id.*

344. Josh Smith, *Bono Mack, Blackburn Introduce Industry-Friendly Cyber Bill*, NAT'L JOURNAL (Mar. 27, 2012, 11:14 AM), http://www.nationaljournal.com/blogs/techdailydose/2012/03/bono-mack-blackburn-introduce-industry-friendly-cyber-bill-27.

Lieberman, Collins, Rockefeller, and Feinstein in response to Majority Leader Reid's instruction that all committees of jurisdiction work together to produce a single piece of legislation.[345] In its original form, CSA (1) authorized DHS to establish baseline mandatory cybersecurity performance requirements for systems in critical infrastructure sectors; and (2) included information-sharing provisions to facilitate private sector sharing of cyberthreat information with other private sector companies and with the government.[346]

CSA's opponents—including many Republicans and industry groups—tendered the standard arguments against cybersecurity regulation, arguing that it would be costly, ineffective, and hamper innovation.[347] Industry opponents also likely harbored concern (albeit rarely expressed) that establishing cybersecurity standards—even minimum baselines standards—would raise the specter of potential tort liability for losses caused by a corporation's failure to meet those standards.

One of the most commonly heard refrains from CSA opponents was that the bill would encourage a culture not of "security," but of "compliance." The Business Roundtable, an association of CEOs of major U.S. companies, stated: "[CSA] would lead to static, prescriptive regulations that do not address dynamic cybersecurity risks and would force companies to shift scarce resources from security to compliance."[348] The Business Roundtable maintained that CSA favored "burdensome and ineffective 'check-the-box' security approaches over sophisticated management of shared cyber risks."[349] Echoing these sentiments, the Telecommunication Industry Association, the lead industry association representing manufacturers and suppliers of global networks, wrote:

> [I]ndustry's primary concern with transitioning to a mandatory regulatory regime . . . . is that imposing rigid regulatory requirements—requirements that by their nature will be unable to keep up with rapidly

345. *Cybersecurity*, U.S. SENATE COMMITTEE ON HOMELAND SECURITY & GOV'T AFF., http://www.hsgac.senate.gov/issues/cybersecurity (last visited Apr. 1, 2013).

346. *See* Cybersecurity Act of 2012, S. 2105 §§ 105, 701–08 (2012).

347. *See* David Inserra, *Cybersecurity Executive Order Touts More Regulation as the Solution*, THE FOUNDRY (Nov. 2, 2012, 1:58 PM), http://blog.heritage.org/2012/11/02/cybersecurity-executive-order-touts-more-regulation-as-the-solution/ ("[R]egulations hinder innovation. Since companies will try to meet outdated cybersecurity regulations, cybersecurity companies will focus on meeting this demand. However, time spent meeting this demand for older cybersecurity approaches is time not being spent innovating ways to fight newer threats.").

348. Letter from Ajay Banga, Chair, Info. & Tech. Comm., Bus. Roundtable, to Harry Reid & Mitch McConnell, U.S. Senators (July 31, 2012), *available at* http://businessroundtable.org/news-center/business-roundtable-letter-on-the-revised-cybersecurity-act-of-2012/.

349. *Id.*

> evolving technologies and threats—would require industry to focus on obsolete security requirements rather than facing the actual threat at hand, effectively making systems *less* secure. Instead, the key to improving the cybersecurity of critical infrastructure is to strengthen the broader cyber ecosystem that enables rapid information sharing, enhances public private partnerships, and provides sufficient investment to address current and emerging threats.[350]

Meanwhile, proponents of CSA viewed the bill as a basic—and long overdue—effort to provide a necessary security framework for private sector companies, particularly those that control critical infrastructure.[351] Under the CSA,

> Company CEOs would only need to certify once a year that they had taken steps to secure their networks, using measurable outcome-based guidelines. DHS would not prescribe how they should do this, but simply define outcomes that a company could then use any technology or technique to achieve. This was very light regulation, but for some it was still too much.[352]

c. Revised Cybersecurity Act

On July 19, 2012, in what was ultimately an unsuccessful attempt to secure Senate passage of their cybersecurity legislation, Senators Lieberman and Collins introduced a revised version of their omnibus cybersecurity bill ("Revised Cybersecurity Act") designed to address Republican concerns. The compromise bill, which the Obama Administration supported, included *voluntary* cybersecurity standards for critical infrastructure,[353] information-sharing provisions,[354] and substantial

350. TELECOMMS. INDUS. ASS'N, *supra* note 282; *see* Inserra, *supra* note 347 ("[R]egulations create a false sense of security and an attitude of compliance. The private sector would follow the regulations and do little more. After all, if it follows the regulations, the government has declared that the private sector is doing cybersecurity right. This will give the private sector the wrong incentive. Instead of promoting the adoption of the most appropriate cybersecurity system, regulations merely encourage the private sector to meet the outdated standards.").

351. CSA reflects the view espoused by some experts that federal government action is necessary to secure the Internet's infrastructure. *See, e.g.*, SPADE, *supra* note 23, at 36 ("The biggest step the federal government can take is to secure the Internet's infrastructure . . . . If the government intends to use the commercial sector for IT, industry security must be federally regulated."). Colonel Spade takes the argument even further, arguing that "SCADA systems must be disconnected from the Internet." In his view, critical infrastructure should then be included in a "federally secured network," which would "allow national utilities to remain linked with greatly reduced vulnerability to CNE [i.e., cyber network exploitation]." *Id.*

352. Lewis, *supra* note 308.

353. *See* Cybersecurity Act of 2012, S. 3414, 112th Cong. § 103; *see also* Jonathan G. Cederbaum et al., *Senate to Consider Compromise Cybersecurity Legislation*,

civil liberties protections.[355]

First, the Revised Cybersecurity Act provided for voluntary standards. To encourage CI owners and operators to adopt the standards, the bill offered an array of incentives. The incentives included liability protection from any punitive damages arising out of a cybersecurity incident if the CI owner/operator was substantially in compliance with the standards at the time of the incident; priority technical assistance for response to cyber threats; and potential access to classified cyberthreat information.[356]

Second, the Revised Cybersecurity Act included revised information-sharing provisions.[357] These provisions required the creation of a federal cybersecurity information exchange led by a civilian agency,[358] and limited the sharing of private-sector provided cyberthreat information with other Federal agencies. In this vein, the bill allows disclosure of cyberthreat indicators to, and use of those indicators by, law enforcement only for specific purposes.[359] The bill also provides liability protection for private sector actors who share information with the government in "good faith" and without "gross negligence."[360]

Critics of the compromise bill described a number of concerns in addition to those typically expressed in prior debates over cybersecurity standards (i.e., cost, hindered innovation, "compliance" over "security," etc.). For example, one critic suggested that "the government will withhold cyber threat and vulnerability information from those private sector actors who do not adopt the [voluntary] standards"[361] and wrote:

WILMERHALE (July 23, 2012), http://wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=10737418914.

354. *See* S. 3414 §§ 701–08.

355. *See, e.g.*, *id.* § 201 (amending the Federal Information Security Management Act to include the civil liberties protections set forth in §§ 3553(b)(1)(G), 3553(e)(2)(A)(ii), and 3554(b)); *id.* § 301 (amending the Homeland Security Act of 2002 by adding Sections 242(d)(4) and 243(a)(4)); *id.* §§ 704(g)(3)–(6). For a detailed analysis of the provisions of the Revised Cybersecurity Act, see Cederbaum et al., *supra* note 353.

356. *See* SENATE COMM. ON HOMELAND SEC. & GOVERNMENTAL AFF., THE REVISED CYBERSECURITY ACT OF 2012 S. 3414 (INTRODUCED JULY 19 2012) (2012), http://www.hsgac.senate.gov/download/cybersecurity-act-of-2012_-revision-two-page-summary; *see also* Paul Rosenzweig, *Thoughts About the Revised Lieberman-Collins Cybersecurity Bill*, LAWFARE (July 21, 2012, 11:20 AM), http://www.lawfareblog.com/2012/07/thoughts-about-the-revised-lieberman-collins-cybersecurity-bill/.

357. S. 3414 §§ 701–08.

358. *Id.* § 703.

359. *Id.* § 704(g)(2).

360. *Id.* § 706(b), (g).

361. Rosenzweig, *supra* note 356.

> It is at least reasonable to ask whether this is the right carrot. Should the government be in the position of denying government threat information to critical infrastructure owners who choose not to adopt the voluntary standards (especially if that decision may be for justifiable business reasons of cost). If the infrastructure in question is truly "critical" it is in America's collective interest to protect them as much as we can. Denying them the informational tools to do so because they don't follow the government's lead may be cutting off our nose to spite our own face.[362]

Another criticism was that the bill did not sufficiently protect companies against liability. Although the bill protects companies from punitive damages if they comply with the standards, one legal scholar claimed that the protections were of little value saying, "I would have argued that even in the absence of an explicit liability protection[,] any company that adopted government approved cybersecurity standards and could show their compliance with them would be immune from punitive damages."[363]

Cybersecurity expert James Lewis criticized the compromise bill for a more fundamental reason. According to Lewis, the bill "simply translates the status quo into legislation—a status quo we all know is inadequate."[364] Lewis explains that the bill "relies on voluntary action—for everyone, regardless of their importance to national security. But what everyone does now is entirely voluntary, and more of the same will not improve security."[365] According to Lewis:

> [The bill] continues the overreliance on information sharing, accompanied by complicated protections to assuage the privacy community. Regulatory agencies can make cybersecurity standards mandatory to the limits of their existing authorities . . . . The bill offers weak incentives for companies to certify that their networks are secure . . . . [and f]ew companies are likely to certify themselves because the incentives in the bill don't compensate for the regulatory risk this creates.[366]

Notwithstanding these criticisms, the White House and many Senators lent their support to the bill. In an unusual move, President Obama signed a July 19, 2012, *Wall Street Journal* op-ed urging the Senate to pass the compromise bill. He argued:

---

362. *Id.*
363. *Id.*
364. Lewis, *supra* note 308.
365. *Id.*
366. *Id.*

> The American people deserve to know that companies running our critical infrastructure meet basic, commonsense cybersecurity standards, just as they already meet other security requirements. Nuclear power plants must have fences and defenses to thwart a terrorist attack. Water treatment plants must test their water regularly for contaminants. Airplanes must have secure cockpit doors. We all understand the need for these kinds of physical security measures. It would be the height of irresponsibility to leave a digital backdoor wide open to our cyber adversaries.[367]

It is important to note that the Senate's compromise bill embraced a voluntary, incentives-based system; precisely the system that the Chamber of Commerce proposed in their March 2011 White Paper and that the House task force endorsed in October 2011.[368] Even so, on August 2, 2012, just weeks before the 2012 election, Senate Republicans blocked the compromise legislation from coming to a vote after "a handful of business lobbying groups and trade associations, most notably the United States Chamber of Commerce," opposed "voluntary" standards.[369] CSA's supporters failed (by a vote of 52-46) to get the sixty votes needed to end debate on the filibustered bill.[370]

On October 13, 2012, just days after then-Defense Secretary's Panetta's "cyber 9/11" speech, Senate Majority Leader Harry Reid vowed to bring the stalled legislation back for Senate consideration during the lame duck session.[371] On November 14, the Senate once again failed to advance the legislation, this time by a vote of 51-47.[372]

---

367. Obama, *supra* note 100.

368. THORNBERRY ET AL., *supra* note 297, at 7–8 ("Congress should encourage participation in the development of voluntary cybersecurity standards and guidance through non-regulatory agencies such as [NIST], to help the private sector improve security. These standards should be developed by a public-private partnership, focus on security best practices, and remain technology-neutral as much as possible. Additionally, the public-private partnership should evaluate which incentives or strategies would increase the adoption of successful security best practices. An example would include varying degrees of liability protections afforded to companies that voluntarily implement the enhanced security practices.").

369. Letter from John D. Rockefeller IV, U.S. Senator, Chairman, Comm. on Commerce, Sci. & Transp., to Virginia M. Rometty, President & C.E.O., IBM (Sept. 19, 2012), *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=396eb5d5-23a4-4488-a67c-d45f62bbf9e5.

370. Sarah Orrick, *Cybersecurity Bill Blocked by Senate Filibuster*, CONG. DIG. (Aug. 3, 2012), http://congressionaldigest.com/cybersecurity-bill-blocked-by-senate-filibuster/.

371. Ben Geman, *Reid Vows Fresh Effort to Pass Stalled Cybersecurity Bill in November*, THE HILL (Oct. 13, 2012, 2:38 PM), http://thehill.com/blogs/hillicon-valley/technology/261891-reid-vows-fresh-bid-to-pass-stalled-cybersecurity-bill.

372. *Bill Summary & Status, 112th Congress (2011-2012), S. 3414*, LIBR. OF CONG. http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.3414: (last visited Apr. 2, 2013).

B. Rockefeller Letter

On September 19, 2012, just weeks after comprehensive cybersecurity legislation was first blocked in the Senate, Senator Rockefeller sent an "unprecedented"[373] letter directly to the CEO of each of the Fortune 500 companies seeking their views on cybersecurity "without the filter of Beltway lobbyists."[374] Senator Rockefeller posed the following eight questions seeking detailed information on corporate cybersecurity practices:[375]

1. Has your company adopted a set of best practices to address its cybersecurity needs?
2. If so, how were these cybersecurity practices developed?
3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.
4. When were these cybersecurity practices developed? How frequently have they been updated? Does your company's board of directors or audit committee keep abreast of developments regarding the development and implementation of these practices?
5. Has the federal government played any role, whether advisory or otherwise, in the development of these cybersecurity practices?
6. What are your concerns, if any, with a voluntary program that enables the federal government and the private sector to develop, in coordination, best cybersecurity practices for companies to adopt as they so choose, as outlined in the Cybersecurity Act of 2012?
7. What are your concerns, if any, with the federal government conducting risk assessments, in coordination with the private sector, to best understand where our nation's cyber vulnerabilities are, as outlined in the Cybersecurity Act of 2012?
8. What are your concerns, if any, with the federal government determining, in coordination with the private sector, the country's most critical cyber infrastructure, as outlined in the Cybersecurity Act of 2012?

Then (in what appears to have been a thinly veiled reference to passage

373. *See* Catherine Dunn, *Ex-IBM Privacy Officer on Preparing for the Future of Cybersecurity*, LAW.COM (Nov. 30, 2012), http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1202578672642&ExIBM_Privacy_Officer_on_Preparing_for_the_Future_of_Cybersecurity&slreturn=20130122101602 (quoting Harriet Pearson, former IBM Chief Privacy Officer and now-partner at Hogan Lovells, describing Rockefeller's letter as "unprecedented").

374. Letter from John D. Rockefeller IV to Virginia M. Rometty, *supra* note 369.

375. *Id.*

of the Patriot Act after 9/11) Senator Rockefeller wrote that the approach taken in the compromise bill "strikes me as one that companies would want to have codified in statute, rather than risking reactive and overly prescriptive legislation following a cyberdisaster."[376] Yet,

> [m]ost observers believe that the United States will only get effective cybersecurity legislation after there has been a crisis and that the country will then overreact, trampling privacy and putting in place rigid requirements. No one on the Hill wants this outcome, but it may be unavoidable. The fate of cybersecurity legislation is symptomatic of a larger political crisis. Congress knows there is a problem, but cannot agree on a fix.[377]

In the absence of a legislative fix in the 2011–2012 session, Senator Rockefeller and others urged President Obama to address cybersecurity through an Executive Order, while many Republicans, including Senator Collins, cautioned the President against doing so.[378]

C. *Executive Order*

> *Whether these [cybersecurity] bills become law or not, the task of finding new, effective ways to secure the country's infrastructure and networks will now revert to the executive branch.*[379]
> *- James A. Lewis, CSIS*

As early as August 2012, press reports suggested that the White House, frustrated by Congress' failure to act on cybersecurity, had begun to entertain the idea of taking executive action.[380] The White House focused its efforts on critical infrastructure protection, the most controversial part of the comprehensive cybersecurity legislation that failed in the Senate, recognizing, of course, that limits on executive authority would constrain its ability to fully implement its policy vision through executive action.[381]

---

376. *Id.*

377. Lewis, *supra* note 308.

378. Eric Chabrow, *'We Can't Wait' for Cybersecurity: Divisions Surface Among Cybersecurity Act Backers*, BANK INFO SECURITY (Sept. 10, 2012), http://www.bankinfosecurity.com/blogs/we-cant-wait-for-cybersecurity-p-1352 ("[A]n Executive Order should not be a substitute for legislative action . . . . An executive order could send the unintended signal that congressional action is not urgently needed.").

379. Lewis, *supra* note 308.

380. Suzanne Kelly, *President Mulling Executive Order to Fill Cybersecurity Gap*, CNN (Aug. 9, 2012, 4:49 PM), http://security.blogs.cnn.com/2012/08/09/president-mulling-executive-order-to-fill-cybersecurity-gap/.

381. *See, e.g.*, CTR. FOR ENERGY & ENVTL. SEC., UNIV. OF COLO. L. SCH., THE BOUNDARIES OF EXECUTIVE AUTHORITY: USING EXECUTIVE ORDERS TO IMPLEMENT FEDERAL CLIMATE CHANGE POLICY 15–21, http://cospl.coalliance.org

Just six weeks after Senate Republicans first blocked comprehensive cybersecurity legislation, the Administration had completed an initial draft of its cybersecurity Executive Order ("EO").[382] A revised draft, dated November 21, surfaced shortly after Senate Republicans blocked passage of compromise cybersecurity legislation on November 14, 2012 during the lame duck session.[383]

Although DHS Secretary Janet Napolitano suggested that the Administration's cybersecurity EO was "close to completion" in late September,[384] the final EO was not signed until February 12, 2013.[385] Some theorized that the Administration was working to "get it right" by reaching out to stakeholders for input. Indeed, according to a White House spokeswoman, by the end of November, "The National Security Staff ha[d] held over 30 meetings with industry, think tanks, and privacy groups, meeting directly with over 200 companies and trade organizations representing over 6,000 companies that generate over $7 trillion in economic activity and employ more than 15 million people."[386] Others conjectured that the *threat* of an EO dealing only with the critical infrastructure problem could open the door for legislative movement on the previously-stalled comprehensive cybersecurity bill.[387] Still others thought

---

/fedora/repository/co:5359 (discussing sources of authority for executive orders); *see also* Brian Prince, *Obama Administration in Talks to Draft Cyber-Security Executive Order*, EWEEK (Nov. 27, 2012), http://www.eweek.com/servers/obama-administration-in-talks-to-draft-cyber-security-executive-order/ (discussing constraints on what executive orders can accomplish).

382. The Administration's draft Executive Order is not to be confused with the administration's Presidential Decision Directive, PDD-20, signed in October or with the draft Presidential Directive on Critical Infrastructure Protection which is designed to update HSPD-7. *See* Nakashima, *supra* note 271. Although initial media reports suggested that a draft of the Administration's Executive Order had been leaked in mid-September, the leaked document was the Presidential Directive updating HSPD-7. *See* Mike Masnick, *LEAKED! Here's the White House's Draft Cybersecurity Executive Order*, TECHDIRT (Sept. 14, 2012, 8:23 PM), http://www.techdirt.com/articles/20120914/19280020390/leaked-heres-white-houses-draft-cybersecurity-executive-order.shtml.

383. Draft Exec. Order, Improving Critical Infrastructure Cybersecurity (Nov. 21 2012), http://www.lawfareblog.com/wp-content/uploads/2012/11/White-House-Draft-Executive-Order-Dated-11-21-12.pdf [hereinafter Draft Exec. Order].

384. *Sen. Rockefeller Asks Fortune 500 CEOs for Cybersecurity Best Practices*, HOMELAND SEC. NEWS WIRE (Oct. 18, 2012), http://www.homelandsecuritynewswire.com/dr20121018-sen-rockefeller-asks-fortune-500-ceos-for-cybersecurity-best-practices.

385. Although signed on February 12, 2013, the EO was embargoed for release until after the February 13, 2013 State of the Union Address.

386. Tony Romm, *Draft Cyber Executive Order Excludes Commercial Products*, POLITICO (Nov. 30, 2012, 3:51 PM), http://www.politico.com/story/2012/11/draft-cyber-executive-order-excludes-commercial-products-84462.html#ixzz2FcFUYVZB.

387. *See* Andy Grotto, Staff Member, Senate Select Intelligence Comm., Speaking

that the Administration held off because it wanted the political cover of failed congressional legislation before issuing the EO.

When the EO was issued, it focused on two major issues: cybersecurity information sharing and the development and implementation of risk-based cybersecurity standards for critical infrastructure.[388]

1. Information Sharing

The EO's information sharing provisions build on existing DoD and DHS information sharing initiatives designed to safeguard critical defense information stored on, or transiting, the privately-owned networks of defense industrial base ("DIB") and, in some cases, CI companies. These initiatives include the DIB Cybersecurity and Information Assurance Program ("DIB CS/IA"), the DIB Exploratory Cybersecurity Initiative ("DIB Pilot"), the DIB Enhanced Cybersecurity Services ("DECS") Program, and the Enhanced Cybersecurity Services ("ECS") Program.

DoD initiated the voluntary DIB CS/IA information sharing program with DIB companies to help safeguard sensitive but unclassified DoD information on DIB unclassified networks.[389] DIB companies participating in the program are required to execute a framework agreement governing their cybersecurity information sharing with the government. Under the DIB CS/IA program, DoD provides "cyber threat information and information assurance best practices to DIB companies,"[390] and in return, DIB participants report to the government "cyber incidents that may involve DoD information" and, participate in cyberintrusion damage assessments as needed.[391] Although the program began with a limited number of DIB participants, DoD subsequently opened the program to all eligible DIB companies[392] and formalized the program through an interim

---

at ABA Section of Science and Technology Law in Washington, D.C. (Dec. 17, 2012).

388. *Compare* Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity § 1, 78 Fed. Reg. 11,737, 11,739 (Feb. 19, 2013) (discussing the policy behind the EO in section one), *with* Draft Exec. Order, *supra* note 383, § 1.

389. Memorandum from Ashton B. Carter, U.S. Deputy Sec'y of Def., on Defense Industrial Base Cyber Security 1 (Oct. 31, 2012), http://www.acq.osd.mil/dpap/policy/policyvault/OSD012537-12-RES.pdf.

390. *Id.*

391. *Id.*; Howard A. Schmidt, *Partnership Developments in Cybersecurity*, WHITE HOUSE BLOG (May 21, 2012, 2:17 PM), http://www.whitehouse.gov/blog/2012/05/21/partnership-developments-cybersecurity.

392. Dep't of Def. Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 77 Fed. Reg. 27,615, 27,621 (May 11, 2012) (codified at 32 C.F.R. § 236) [hereinafter DIB CS/IA Program] (setting forth DIB participant eligibility requirements); Press Release, U.S. Dep't of Def., DoD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities (May 11, 2012), *available at* http://www.defense.gov/releases/release.aspx?releaseid=15266.

final rule issued May 11, 2012.[393]

The DIB CS/IA program includes an optional component known as DIB ECS ("DECS").[394] DECS specifically addresses the need to share *classified* threat information and signatures with DIB companies participating in the DIB CS/IA. Specifically, under the DECS program, the government (i.e., NSA) provides "classified cyber threat and technical information either to a DIB company or to the DIB company's Commercial Service Provider [("CSP")]."[395] DECS was based on "lessons learned" from a DoD pilot program, known as the DIB Pilot, that started back in July 2010. The DECS program ultimately became a joint DoD-DHS program "falling under the umbrella" of DHS's Enhanced Cybersecurity Services ("ECS") program[396] with DHS taking the leadership role.

The first phase of ECS "focused on the cyber protection of the DIB companies participating in DoD's [DIB CS/IA]."[397] By January 2013, DHS had decided to expand ECS to provide "enhanced cybersecurity protection" to *all U.S. CI sectors* through "the sharing of indicators of malicious cyber activity with CSPs."[398]

The success of the DIB Pilot, DECS, and ECS is unclear. While some view these programs as "an important step forward in our ability to catch up with widespread cyberthreats,"[399] others have expressed concern that "[t]he DIB pilot probably increases the defenders' work factor much more than it increases the attackers."[400] An independent review of the DIB Pilot[401] found that the program had only "marginal benefit."[402]

---

393. DIB CS/IA Program 77 Fed. Reg. 27,615.

394. DIB ENHANCED CYBERSECURITY SERVICES (DECS), http://www.dc3.mil/dcise/DIB%20Enhanced%20Cybersecurity%20Services%20Procedures.pdf.

395. Memorandum from Ashton B. Carter, *supra* note 389, at 1.

396. In January 2012, DHS and DoD announced that they would be undertaking a proof of concept known as the Joint Cybersecurity Services Pilot ("JCSP"). Under the JSCP, operational relationships with CPSs in the DIB Pilot were shifted from DoD to DHS. JCSP subsequently became known as the Enhanced Cybersecurity Services (ECS) program. *E.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE ENHANCED CYBERSECURITY SERVICE (ECS), DHS/NPPD/PIA-028 2 (2013), http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.

397. *Id.* at 2.

398. *Id.*

399. Taylor Armerding, *Will Voluntary Cyber Threat Sharing Plan Case Doubt Over CISPA?*, NETWORKWORLD (May 18, 2012, 9:20 AM), http://www.networkworld.com/news/2012/051812-will-voluntary-cyber-threat-sharing-259423.html (quoting Richard A. Hale, deputy chief information officer for cybersecurity at the NSA).

400. *Id.* (quoting Jay Healey, director of the Cyber Statecraft Initiative at Atlantic Council, a Washington, D.C. think tank).

401. *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber*

The EO builds on existing information sharing programs in several ways. First, the EO confirms that it is U.S. policy to improve cybersecurity information sharing, specifically by increasing the "volume, timeliness, and quality" of cyberthreat information shared with the U.S. private sector.[403] Second, the EO puts the President's imprimatur on the planned expansion of ECS to CI sectors. Specifically, the EO directs DHS and DoD to establish procedures to expand ECS to all CI sectors within 120 days.[404] Third, pursuant to the EO, unclassified versions of reports of cyberthreats to the United States that identify a specific target must be rapidly disseminated to the target.[405]

The EO also encourages the private sector to share information with the government. Toward this end, the EO provides that "[i]nformation submitted voluntarily . . . by private entities under this order shall be protected from disclosure to the fullest extent permitted by law."[406] However, private sector companies may remain reluctant to share information with the government due to the EO's lack of liability protections. The White House did not have the authority to provide liability protections through an executive order; an act of Congress is required.[407] Indeed, legislation may be necessary to address a number of

---

Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program Before the S. Comm. on Armed Services, 112th Cong. 1–3 (2012) (opening statement of Carl Levin, U.S. Senator), http://www.armed-services.senate.gov/Transcripts/2012/03%20March/12-19%20-%203-27-12.pdf [hereinafter *Hearing Testimony in Review of Defense Authorization 2013*] ("Carnegie Mellon conducted an independent assessment of the DIB Pilot for DoD.").

402. Armerding, *supra* note 399 (noting that only "1% of attacks [were] . . . detected using NSA threat data that the companies did not already have themselves," according to Jay Healey, director of the Atlantic Council's Cyber Statecraft Initiative); *Hearing Testimony in Review of Defense Authorization 2013*, *supra* note 401, at 3 (opening statement of Carl Levin, U.S. Senator) ("Carnegie Mellon concluded [based on their independent assessment] that NSA provided few signatures that were not already known to the companies themselves, and in many cases, the DIB companies by themselves detected advanced threats with their own non-signature-based detection methods that probably [were] not known to the NSA."); Jason Healey, *Cybersecurity Legislation Should Force U.S. Government to Listen Less and Speak More*, THE ATLANTIC (Mar. 15, 2012, 5:21 PM), http://www.theatlantic.com/technology/archive/2012/03/cybersecurity-legislation-should-force-us-government-to-listen-less-and-speak-more/254491/ ("[NSA's signature database is] considered among the crown jewels of the U.S. government's defense capabilities [but] may not be as awe-inspiring as advertised.").

403. Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity §§ 1, 4(a), 78 Fed. Reg. 11,737, 11,739 (Feb. 19, 2013).

404. *Id.* § 4(c), at 11,739–40.

405. *Id.* § 4(b), at 11,739.

406. *Id.* § 5(d), at 11,740.

407. Eric Chabrow, *Exec Order Could Ease Cybersecurity Bill Passage: Ridding Gov's Role in Setting Standards from Legislative Equation*, BANK INFO SECURITY (Dec.

issues surrounding information sharing, including the controversial privacy and civil liberties implications of such sharing.[408]

2. Cybersecurity Framework

In addition to information sharing, the EO calls for the collaborative development and voluntary adoption of a new cybersecurity framework to include risk-based cybersecurity standards for critical infrastructure.[409] The EO directs NIST to "lead the development of a framework to reduce cyber risks to critical infrastructure ("Cybersecurity Framework");"[410] to engage in an "open public review and comment process;"[411] and to publish a final version of the Cybersecurity Framework within one year.[412] The EO directs that the Cybersecurity Framework shall include "standards, methodologies, procedures, and processes that align policy, business, and technology approaches to address cyber risk."[413] The EO requires the Cybersecurity Framework to incorporate voluntary consensus standards and industry best practices to the fullest extent possible.[414]

With an eye toward encouraging—rather than impeding—a competitive market, the EO addresses several of the concerns that industry had voiced over voluntary standards. For example, the EO clarifies that "the Cybersecurity Framework will provide [cybersecurity] guidance that is technology neutral,"[415] will not pick technological winners and losers, and will thereby "enable . . . [CI] sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks."[416]

The EO directs DHS to "establish a voluntary program to support the adoption of the Cybersecurity Framework [by CI owners and

---

7, 2012), http://www.bankinfosecurity.com/exec-order-could-ease-cybersecurity-bill-passage-a-5341.

408. *See id.* ("The more contentious matters dealing with information sharing, which also includes protecting the privacy and civil liberties of citizens whose personal information could be exposed during exchanges of data between business and government, must be addressed by legislation.").

409. Exec. Order No. 13,636 § 7(b), 78 Fed. Reg. at 11,739; Chabrow, *supra* note 407 ("At the heart of the proposed executive order is a process in which the federal government . . . would collaborate with industry to establish IT security best practices that [CI owners] . . . could adopt voluntarily.").

410. Exec. Order No. 13,636 § 7(a), 78 Fed. Reg. at 11,740–41.

411. *Id.* § 7(d), at 11,741.

412. *Id.* § 7(e), at 11,741.

413. *Id.* § 7(a), at 11,740–41.

414. *Id.*

415. *Id.* § 7(b), at 11,741.

416. *Id.*

operators]."[417] The EO explores greater use of "carrots," in the form of incentives, to promote industry participation. Indeed, it "directs the Treasury and Commerce Departments to recommend a set of possible incentives that would entice operators of critical infrastructure to join a voluntary program in which they would follow a set of cybersecurity standards."[418] The EO further directs that DHS, Treasury, and Commerce identify which incentives are available under existing law and which require legislation.[419]

The EO also seeks recommendations regarding the potential use of federal purchasing power to influence adoption of cybersecurity standards. Specifically, the EO directs DoD and the General Services Administration ("GSA"), in consultation with DHS and the Federal Acquisition Regulatory Council, to make recommendations to the President regarding the "feasibility, security benefits, and relative merits" of "incorporating security standards into acquisition planning and contract administration" as well as steps that can be taken "to harmonize . . . existing procurement requirements related to cybersecurity."[420]

In summary, the EO facilitates information sharing and the development and adoption of cybersecurity standards by CI owners and operators. Some congressional leaders fear (and some industry groups are hopeful) that the executive order sends a signal that congressional action is not urgent.[421] However, others believe that by addressing the issue of cybersecurity standards for CI owners and operators, the EO potentially removes from the legislative debate the very issue that prompted Republicans to block the compromise cybersecurity bill, and may therefore pave the way for congressional action on cybersecurity legislation in 2013.[422]

D. Congressional Action (2013)

1. U.S. House of Representatives

a. CISPA

On February 13, 2013, immediately after the EO was issued, HSPCI Chairman Rogers re-introduced CISPA.[423] CISPA passed out of committee on April 10, 2013, after a closed-door debate during which six amendments

417. *Id.* § 8(a), at 11,741.
418. *Id.*
419. *Id.*
420. *Id.* § 8(e), at 11,741.
421. *Cf.* Kelly, *supra* note 378.
422. *See* Chabrow, *supra* note 407.
423. H.R. 624, 113th Cong. (2013).

to the bill—including several amendments designed to strengthen the bill's privacy and civil liberties protections—were approved.[424] The bill's sponsors subsequently took the position that, as amended, CISPA provides appropriate protections for privacy and civil liberties.[425] Many privacy and civil liberties advocates vehemently disagreed,[426] and on April 16, 2013, just days before CISPA reached the House floor for a vote, the White House issued a veto threat, explaining that "if the bill, as currently crafted, were presented to the President, his senior advisors would recommend that he veto the bill."[427] The White House explained that "[w]hile there is bipartisan consensus on the need for . . . [cybersecurity information sharing] legislation, it should adhere to the following priorities: (1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections."[428] The House passed CISPA by a vote of 288-127 on April 18, 2013, just days after the Boston Marathon bombings, with Rep. Mike McCaul (R-Tex.) stating at the House hearing:

> "In the case of Boston, they were real bombs. In this case, they're digital bombs. These bombs are on their way. That's why this legislation is so urgent. For if we don't and those digital bombs land and attack the

424. Press Release, U.S. House of Representatives Permanent Select Committee on Intelligence, Bipartisan Cybersecurity Bill Clears Key Hurdle, April 10, 2013, http://intelligence.house.gov/press-release/bipartisan-cybersecurity-bill-clears-key-hurdle-0. For a textual version of the bill and its amendments, see *H.R. 624 - The Bill and Amendments*, U.S. HOUSE OF REP. PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/hr-624-bill-and-amendments (last visited May 3, 2013).

425. *Myths and Facts about the Cyber Intelligence Sharing and Protection Act (CISPA)*, http://www.dutch.house.gov/CISPA%20MYTHBUSTER%202013.pdf; *see Cyber Intelligence Sharing and Protection Act of 2013*, U.S. HOUSE OF REP. PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/CivilLibertiesTPsCyberBillFeb112013v2.pdf.

426. For example, the American Civil Liberties Union decries CISPA's continued (1) lack of civilian control over domestic cyber programs; (2) failure to limit the sharing of personal information; and (3) "unlimited immunity" for hack backs. Michelle Richardson, *CISPA Remains Fatally Flawed After Secret Committee Markup*, AM. CIVIL LIBERTIES UNION (Apr. 12, 2013, 12:20 PM), http://www.aclu.org/blog/technology-and-liberty-national-security-free-speech/cispa-remains-fatally-flawed-after-secret ("We have flagged four general categories of problems in CISPA that have to be fixed before it is passed, and the markup only substantially fixed one of them . . . .").

427. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 624 – CYBER INTELLIGENCE SHARING AND PROTECTION ACT (2013), http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf.

428. *Id.*

United States, and Congress failed to act, then Congress has that on [its] hands."[429]

b. SECURE-IT Act

On April 10, 2013, Rep. Marsha Blackburn (R-Tenn.) re-introduced the SECURE-IT Act in the House.[430]

2. U.S. Senate

On the Senate side, Senators Tom Carper, John D. Rockefeller IV, and Diane Feinstein introduced the Cybersecurity and American Cyber Competitiveness Act of 2013[431] on January 23, 2013. Despite its impressive title, the legislation is nothing more than a "sense of Congress" that there *should* be legislation.[432] In his press release announcing the bill, Senator Carper stated: "It is a priority this year to act on comprehensive cybersecurity legislation."[433]

Senator Feinstein has since announced her intention to introduce information sharing legislation through the Senate Intelligence Committee, which she chairs.[434]

E. Regulatory Litigation

Recent regulatory litigation developments, such as *Federal Trade Commission ("FTC") v. Wyndham*, should inform corporate cybersecurity investments.[435] *Wyndham* marks the first time that the FTC has sued a major company in federal court for failure to *secure* customer information. The FTC's suit alleges that Wyndham and its subsidiaries had flawed security practices (including failure to erect firewalls, use appropriate

429. Elizabeth Flock, *Texas Congressman Uses Boston Bombing to Argue for CISPA Passage*, U.S. NEWS & WORLD REPORT (Apr. 18, 2013), http://www.usnews.com/news/blogs/washington-whispers/2013/04/18/texas-congressman-uses-boston-bombing-to-argue-for-cispa-passage.

430. H.R. 1468, 113th Cong. (2013).

431. S. 21, 113th Cong. (2013).

432. *Id.* § 3.

433. Press Release, Tom Carper, U.S. Senator, Comprehensive Cybersecurity Bill Will Be Priority this Congress (Jan. 23, 2013), *available at* http://www.carper.senate.gov/public/index.cfm/pressreleases?ID=99646255-b703-4647-96e5-c1c4e9fdc1a4.

434. Katy O'Donnell, *Intelligence Leaders: Cybersecurity Now the Top Global Threat*, MAIN JUST. (March 13, 2013, 9:38 AM), http://www.mainjustice.com/2013/03/13/intelligence-leaders-cybersecurity-now-the-top-global-threat/ (quoting Senator Feinstein saying that she and Senator Chambliss will begin an effort shortly to "see if we can't get a bill that we can agree to move through the [Senate Intelligence] committee on the information-sharing part of it.").

435. Complaint, FTC v. Wyndham Worldwide Corp., filed (D. Ariz. 2012) (No. 2:12-cv-01365-SPL), http://ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf.

passwords, or configure software to keep credit card information secure).[436] FTC officials have called the alleged security flaws "obvious."[437]

In the *Wyndham* complaint, the FTC claims that Wyndham's security practices constitute both unfair and deceptive practices in violation of the FTC Act. First, the FTC alleges that Wyndham's failure to safeguard personal information caused substantial consumer injury and constituted an unfair practice. Second, the FTC alleges that Wyndham's privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers' personal information.[438] The FTC alleges, for example, that Wyndham failed to keep up with industry cybersecurity standards despite promising to do so in its own privacy policy.[439]

In *Wyndham*, the FTC essentially is asserting that it can use its enforcement authority to hold companies to their data security promises, including promises to adopt "reasonable security measures." As the FTC litigates more of these cases, a body of legal rulings is likely to develop regarding the meaning of "reasonable security."[440] Such rulings potentially could eventually serve as a basis for tort liability (i.e., liability for failure to take reasonable security measures), which likely explains why the U.S. Chamber of Commerce, through the National Chamber Litigation Center, has filed an amicus brief on behalf of the defendants in *Wyndham*, urging the Court to grant Wyndham's motion to dismiss.[441]

Wyndham also serves as a cautionary tale, reminding corporations of the care that must be taken when drafting corporate data security policies governing the handling of consumer information. It is imperative that corporations ensure that their data security policies accurately describe their data security practices and make only those promises that the

436. *See id.* at 10.

437. Craig Timberg, *FTC Sues Wyndham Hotels over Hacker Breaches,* WASH. POST (June 26, 2012), http://articles.washingtonpost.com/2012-06-26/business/35459761_1_hackers-personal-data-information-security.

438. Complaint at 17, *Wyndham Worldwide Corp.*, (No. 2:12-cv-01365-SPL).

439. *Id.* at 18–19.

440. In a recent non-regulatory litigation that may signal the "future of business-to-business litigation," according to Crowell & Moring LLP partner David Bodenheimer, an Oregon company reportedly sued its bank to recover nearly a quarter of a million dollars that cyberthieves stole from its accounts. The company reportedly alleged that the bank violated the requirements for commercially reasonably security procedures set forth in Uniform Commercial Code Section 4A. Brian Krebbs, *Hay Maker Seeks Cyber Heist Bale Out*, KREBS ON SECURITY, April 13, 2013, http://krebsonsecurity.com/2013/04/hay-maker-seeks-cyberheist-bale-out/; *see* Complaint at 1, Oregon Hay Prod., Inc. v. Cmty. Bank (Or. Cir. Ct.) (No. CVH120083).

441. *See* Brief for U.S. Chamber of Commerce et al. as Amici Curiae Supporting Defendants, FTC v. Wyndham Worldwide Corp., filed (D. Ariz. 2012) (No. 12-1365-SPL).

corporation can and will keep.

VI. PRIVATE SECTOR CHALLENGES

The basic problem—true since 1998—is there are no incentives sufficient to make companies in most critical infrastructure sectors take voluntary action to bring the security of their networks to the level needed for national defense.
- James A. Lewis, CSIS[442]

A. The Limits of Vulnerability Mitigation

The U.S. self-regulatory approach to ".com" cybersecurity has long been heavily focused on vulnerability mitigation. Behind the fancy language is a simple idea: that by strengthening our cyberdefenses we will better protect the ".com" domain against cyberthreats, including cybercrime, cyberespionage, and cyberwar. Yet, by all accounts, it appears that we remain quite vulnerable to cyberthreats.

Many experts believe that our continued vulnerability stems from chronic private sector underinvestment in cyberdefenses, particularly with respect to critical infrastructure.[443] Some companies simply fail to make investments in even the basic vulnerability mitigation measures necessary to protect against the cyberthreats posed by "script-kiddies" and run-of-the-mill cybercriminals.[444] Other companies may invest in cyberdefense to protect their own assets, but their investments rarely reflect the fact that, as the nation becomes increasingly interconnected, one company's vulnerabilities may result in harm to another company—or even the nation. As cybercrime, cyberespionage, and cyberwar proliferate, the consequences of inadequate cyberdefenses will only mount.

More fundamentally, in some contexts, our nation's focus on vulnerability mitigation may be misplaced. While good cyberdefenses may be sufficient to ward off certain cyberthreats (e.g., opportunistic cybercrimals), they likely will be insufficient to keep determined adversaries, such as nation-state actors, from perpetrating cyberespionage or cyberwar. This problem will only be exacerbated as malware "trickles down"[445] from nation-state actors to cybercriminals,[446] and as hacking tools

442. Lewis, *supra* note 308.

443. *See* Letter from Michael Chertoff et al. to Harry Reid & Mitch McConnell, *supra* note 182.

444. Panetta, Remarks on Cybersecurity, *supra* note 223 ("[T]he reality is that too few companies have invested in even basic cybersecurity.").

445. Robert Bigman, *Guest Blog: Former CIA CISO on Nation-State Security Challenges*, FIREEYE BLOG (June 15, 2012), http://blog.fireeye.com/research/2012/06/former-cia-ciso-national-security.html ("[A]dditional attacks (mostly kernal rootkits) have appeared that reflect the 'trickle down' of APT technology from nation-states to

are commoditized.

Accordingly, it may be worthwhile to view vulnerability mitigation as but one part of a more holistic ".com" cybersecurity strategy that seeks not only to defend cyberspace, but also to deter threat actors. Today, nation-states and nation-state sponsored actors engaged in cyberespionage face few, if any, consequences for their actions. The U.S. private sector could play an important role in shifting the focus of cybersecurity efforts toward threat deterrence, potentially through its own actions, and also by encouraging the U.S. government to explore ways to bring all elements of national power—including economic, diplomatic,[447] and military—to bear on the evolving cyberthreat.

B. Obstacles to Effective Vulnerability Mitigation

According to experts, one of the key challenges to vulnerability mitigation is the difficulty of spurring adequate private sector investment in cyberdefense, a difficulty that may stem from a variety of sources, including the widely-acknowledged lack of reliable cyberincident data;[448] the "it can't happen to me" mentality evidenced by some corporations; and the "public good" nature of cybersecurity.

---

the cybercriminal industry . . . . [T]he Chinese government engaged cybercriminals to assist in the development and peer review of the Aurora attack code and even shared the final product with them.").

446. Matthew J. Schwartz, *7 MiniFlame Facts: How Much Espionage Malware Lurks?*, INFORMATIONWEEK (Oct. 17, 2012, 12:56 PM), http://www.informationweek.com/security/management/7-miniflame-facts-how-much-espionage-mal/240009237 ("Another worry from nation states' malware espionage operations is that their tricks will soon be put to use by criminals. In a 2009 report on malware used for surveillance purposes, Cambridge University researchers Shishir Nagaraja and Ross Anderson wrote, 'What Chinese spooks did in 2008, Russian crooks will do in 2010 and even low-budget criminals from less developed countries will follow in due course.' In other words, how long will it be until today's Flame [cyberattack malware] becomes the inspiration for tomorrow's financial malware attack?").

447. *See, e.g.*, Press Release, Kirsten Gillibrand, U.S. Senator Gillibrand Announces New Cybersecurity Bill Includes Measures She Authored to Combat Global Cyber Criminals (Feb. 15, 2012), *available at* http://www.gillibrand.senate.gov/newsroom/press/release/gillibrand-announces-new-cybersecurity-bill-includes-measures-she-authored-to-combat-global-cyber-criminals ("[The new bill] authorize[es] a State Department official to coordinate U.S. diplomatic strategy to combat cybercrime and establish a consistent foreign policy when it comes to cybercrime issues across relevant federal departments, agencies, U.S. embassies, and consulates.").

448. Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, DAEDALUS, Fall 2011, at 70, 73, http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf ("[The] lack of information about vulnerabilities, incidents, and attendant losses makes actual risk calculations difficult.").

1. Lack of Cyberincident Data Necessary to Calculate ROI

Executives understandably may be reluctant to invest in cybersecurity without a clear understanding of the return on investment ("ROI")[449] for their cybersecurity dollar because cybersecurity is expensive and can easily become a "black hole"[450] for spending. Unfortunately, the industry lacks reliable ROI data upon which to build a business case for increased cyber defense investments.

Reliable ROI data depends on reliable data about the frequency of cyberincidents, the costs of cyberincidents, and the effectiveness of mitigation methods. Reliable cyberincident information is lacking, both because corporations may be victimized without their knowledge,[451] and because corporations may be reluctant to report cybersecurity breaches,[452] for fear of repercussions in terms of compromised cybersecurity, competitiveness, regulatory risk, consumer response, cost, and/or reputation.[453] Without reliable data about the frequency of cyberincidents, it is difficult for companies to calculate the probability with which

449. *See* Simon Moffatt, *Information Security: Why Bother?*, INFOSEC ISLAND (Dec. 9, 2012), http://www.infosecisland.com/blogview/22774-Information-Security-Why-Bother.html ("Organisations have finite budgets which will cover all of IT and related services, and it is a fair objective, to have to show and prove, either via tangible or intangible RoI, that a piece of software or consultancy will have a beneficial impact on the organisation as a whole.").

450. Erik Sherman, *Hackers Target Small Businesses*, CBS NEWS: MONEYWATCH (July 6, 2012, 11:05 AM), http://www.cbsnews.com/8301-505124_162-57467265/hackers-target-small-businesses/.

451. ALPEROVITCH, *supra* note 96, at 2 ("I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact."); Kellermann, *supra* note 142 ("55% of our customers had to be *informed* that they had a breach versus actually being aware themselves.") (emphasis added); Perlroth, *supra* note 111 (experts say the majority of cyberattacks go "undisclosed or unnoticed"); Andrea Shalal-Esa, *Scores of U.S. Firms Keep Quiet About Cyber Attacks*, REUTERS (June 13, 2012, 3:08 PM), http://www.reuters.com/article/2012/06/13/net-us-media-tech-summit-cyber-disclosur-idUSBRE85C1E320120613 (" '[M]any corporations were unaware that their networks had been breached until FBI agents notified them that they discovered proprietary, company-specific data outside their networks,' [according to Shawn Henry, the FBI's 'former top cyber cop.'] ").

452. Shalal-Esa, *supra* note 451 (" 'There have been lots of breaches in every industry that have never been publicized,' said Shawn Henry . . . .").

453. *See* Gorman & Tibken, *supra* note 162 (" 'It would have been better if RSA was more forthright from the beginning [of their breach]. They unnecessarily damaged their reputation by holding back,' said [one] Gartner analyst . . . . [RSA CEO Art Coviello] said his company has provided the right amount of information to its customers. Providing any further information, he said, would give the hackers a blueprint for how to mount further attacks."); *CF Disclosure Guidance*, *supra* note 288 (discussing concerns that detailed corporate cyberincident disclosures could provide a "roadmap" for adversaries seeking to compromise corporate network security).

cyberincidents are likely to strike. Similarly, reliable information about both the tangible and intangible costs associated with cyberincidents is lacking, not only because corporations are reluctant to report cyberincidents, but also because of the practical difficulty of measuring certain costs, including opportunity costs and the costs associated with reputational harm, loss of consumer confidence, intellectual property loss, and loss of consumer privacy.[454] Finally, the effectiveness of mitigation methods is unknown.

Despite the importance of reliable cyberincident data, a recent survey of 1000 publicly-traded companies revealed that "[fifty-two] percent failed to report . . . network breaches."[455] Experts believe that many corporations fail to report cyberincidents, despite reporting obligations under data breach notification laws and other applicable disclosure rules, such as the SEC's cybersecurity guidance. One cybersecurity expert points to the telling example of a publicly traded defense contractor whose IP was exfiltrated to China as a result of a cyberintrusion. The company decided not to disclose the intrusion and, as justification for its decision, stated that the company "only do[es] business with the U.S. government and it doesn't really matter that the Chinese stole all their IP because the U.S. government will never buy from China, so it wasn't really material to them."[456] So long as companies continue to withhold cyberincident data, obtaining reliable calculations of ROI for cyberdefense spending will remain problematic.

2. "It Can't Happen to Me" Mentality

Whether due to lack of cyberincident data or otherwise, some companies view themselves as immune from cyberthreats. Consider the case of small- and medium-sized businesses ("SMBs"). SMBs are attractive cyber targets because they traditionally have weaker cyberdefenses than larger businesses due to resource constraints.[457] Attacks on SMBs recently accelerated, with the number of targeted attacks against SMBs doubling in the last half of 2012.[458] Moreover, companies with 100 or fewer employees

454. *See generally* ANDERSON ET AL., *supra* note 139 (discussing the difficulties of precisely measuring indirect losses from cybercrime, such as loss of consumer confidence). Estimating cyberespionage costs is also difficult as "there is no reliable data available." *See id.* (criticizing a UK report in which "the authors admit the proportion of IP actually stolen cannot currently . . . be measured with any degree of confidence, so they assign probabilities of loss and multiply by sectoral GDP").

455. Shalal-Esa, *supra* note 451 (citing 2011 SAIC study).

456. *See id.*

457. *See* Sherman, *supra* note 450 (describing SMBs as "perfect prey" because they "tend to lack the resources to fully secure their computer systems," yet they also tend to have "significant amounts of money").

458. Andy Singer, *SMBs—the Weakest Link in the Cybercriminal Supply Chain?*, SYMANTEC (July 10, 2012), http://www.symantec.com/connect/blogs/smbs-weakest-

were the victims in sixty-three percent of data breaches Verizon analyzed in a 2010 study.[459]

Despite their vulnerability, some SMBs have failed to take even the most basic corporate security steps. For example, nearly ninety percent of SMBs have no formal internet security policy and nearly seventy percent lack even an informal policy, according to a recent survey jointly conducted by the National Cyber Security Alliance ("NCSA") and global security solutions provider Symantec.[460] Nearly sixty percent of SMBs do not even have a backup plan in case of a data breach, notwithstanding the significant costs associated with such breaches.[461]

On the whole, the SMBs surveyed by NCSA/Symantec are surprisingly unconcerned about cybersecurity. According to the survey: (1) over eighty percent of SMBs are satisfied with the amount of data security they provide and think they are investing adequate resources in cybersecurity;[462] (2) seventy-seven percent said that their companies are safe from cyberthreats including hackers, breaches, viruses, and malware;[463] and (3) sixty-six percent of SMBs are not concerned about an external or internal cybersecurity threat.[464] Moreover, seventy percent said they have no employee social media usage policy despite the fact that social media can leave businesses more vulnerable to phishing and other social-engineering

---

link-cybercriminal-supply-chain ("[T]here appears to be a direct correlation between a rise in attacks against small companies and a drop in attacks against larger ones, which could mean that attackers are diverting resources directly from one group to the other. Even though larger businesses (2500+ employees) continue to be the primary target for most targeted attacks . . . the gap between the two is quickly closing.").

459. Sherman, *supra* note 450.

460. Press Release, Symantec, New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have no Policies or Contingency Plans (Oct. 15, 2012), *available at* http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01.

461. *Id.*; *Ponemon Study Shows the Cost of a Data Breach Continues to Increase*, PONEMON (Jan. 25, 2012), http://www.ponemon.org/news-2/23 (noting that in a study of forty-five data breach cases, the most expensive data breach cost the affected company $31 million to resolve; the least expensive cost $750,000, emphasizing that most of the costs are from legal defense spending).

462. NAT'L CYBERSECURITY ALLIANCE & SYMANTEC, 2012 NATIONAL SMALL BUSINESS STUDY (2012) http://www.staysafeonline.org/download/datasets/4393/2012_ncsa_symantec_small_business_study_fact_sheet.pdf.

463. *Id.*; *Small Business Online Security Infographic*, STAYSAFEONLINE.ORG, http://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic (last visited Apr. 2, 2013).

464. Scott Cornell, *SMBs in the U.S. Are Soft on Cybersecurity*, FARONICS (Nov. 6, 2012), http://www.faronics.com/2012/smbs-in-the-u-s-are-soft-on-cybersecurity/; Press Release, Symantec, *supra* note 460 ("Visa Inc. reports that small businesses represent more than 90 percent of the payment data breaches reported to the company.").

based cyberincidents.[465]

This "it can't happen to me" mentality has the potential to lead to particularly grave consequences in the current environment, where bad actors are increasingly setting their sights on corporations "low down in the security supply chain as a stepping-stone, with the expectation that they will have less robust security features in place than the top-tier defense contractors or government agencies they ultimately want to target."[466] Today's environment necessitates greater awareness of cyberthreats among SMBs, as well as the companies they supply.

3. "No Corporation Is An Island": Cybersecurity as a Public Good

According to many experts, another key challenge to achieving optimal (or even adequate) private sector investment in cyberdefenses is the fact that cybersecurity is a public good.[467] One company's underinvestment in cyberdefense can redound to the detriment of other companies with whom they connect. Indeed, "a single compromised system anywhere in a network can serve as a launching point for attack on other systems connected to that network."[468] Some companies—e.g., SMBs—may be motivated to invest sufficiently to protect their own assets, but are unlikely to invest sufficiently to protect the assets of companies with whom they do business, leading some experts to conclude that "the private sector will not supply adequate cybersecurity on its own; it's a public good that's missing as the result of market failure."[469] As our interconnectedness grows, the problem is only exacerbated.

---

465. NAT'L CYBERSECURITY ALLIANCE & SYMANTEC, *supra* note 462; *Small Business Online Security Infographic*, *supra* note 463.

466. Ben Weitzenkorn, *'Aurora' Google Hackers Still an Active Threat, Report Says*, TECHNEWSDAILY, (Sept. 10, 2012, 2:37 PM), http://www.technewsdaily.com/8090-aurora-google-hackers-active-threat.html; *see* Singer, *supra* note 458 ("[W]hile your business may not be the primary target of an attack, cybercriminals may be using your organization as a stepping-stone to attack other businesses . . . SMBs typically don't have the resources to maintain a full IT staff, so [they] could be seen as a weaker link in the supply chain.").

467. Mulligan & Schneider, *supra* note 448, at 75 ("Cybersecurity is non-rivalrous and non-excludable; by definition, it is a *public good.* It is non-rivalrous because one user benefiting from the security of a networked system does not diminish the ability of any other user to benefit from the security of that system. And it is non-excludable because users of a secure system cannot be easily excluded from benefits security brings.") (emphasis in original); *see* Bruce H. Kobayashi, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goals* 5 (Geo. Mason Univ. Sch. of L., Working Paper Series, Paper 26, 2005), *available at* http://law.bepress.com/gmulwps/gmule/art26.

468. Mulligan & Schneider, *supra* note 448, at 74.

469. David Perera, *Lewis: Common Assumptions About Cybersecurity Are Wrong*, FIERCEGOVERNMENTIT (Sept. 28, 2011), http://www.fiercegovernmentit.com/story/lewis-common-assumptions-about-cybersecurity-policy-are-wrong/2011-09-28.

Moreover, when companies calculate their optimal level of investment in cybersecurity, they consider their own risks (e.g., risk of IP loss from an intrusion and the cost of such loss), but not the broader set of potential risks, including not only risks to other companies with whom they are connected, but the potential societal risks to our nation's economic or national security from successful cyberespionage or cyberattack. Companies invest in cybersecurity to protect their own assets from cyberthreats, but their investments are unlikely to account for the potential harm to our economic or national security in the event of a cyberincident. Specifically, "[c]ompanies assess the probability that a threat will become an attack, and if there is an attack, whether they will be held liable. They weigh the cost of preventive measures against the risk of liability. Almost all conclude that the liability risk for cyberattack is too low to justify greater effort. This is a sensible business decision but does not help national security."[470]

C. *Failure of Vulnerability Mitigation in the Face of Determined Adversaries*

While there are many challenges to effectively mitigating vulnerabilities, more fundamentally, our nation's focus on cybersecurity through vulnerability mitigation may be misplaced. It has become apparent from the trajectory of both cybercrime and cyberespionage losses that even sophisticated corporate vulnerability mitigation efforts do not thwart the most concerted adversaries (e.g., nation-state adversaries, terrorists, sophisticated cybercriminals, and hacktivists). Even organizations with highly sophisticated cybersecurity programs (e.g., DoD, RSA Security, Lockheed Martin, and Google) are not immune from successful penetration by determined adversaries.

Vulnerability mitigation may be failing against determined adversaries because, when it comes to sophisticated cybersecurity, the offense (i.e., threat actor) currently has a substantial advantage over the defense (i.e., cyberdefender).[471] Offense is cheaper, more agile,[472] better organized,[473]

470. Lewis, *supra* note 308.

471. Some simple examples demonstrate this point. First, it only takes "a couple hundred lines of code to . . . sneak . . . something out of somebody's network," but it can take "at least a million lines of code to patch [the vulnerability]" and there is "more area to attack with every patch. . . . Everything is in the favor of the attacker." James E. Cartwright, General (Retired), Address at the Center for Strategic and International Studies, Global Security Forum 2012: Fighting a Cyber War (Apr. 11, 2012), http://csis.org/files/attachments/120411_FightingACyberWar_GSF_Transcript.pdf. Moreover, if there are twenty vulnerabilities in a networked information system, the offense needs to exploit only one to be successful while the defense may need to find and patch all twenty to successfully keep out a determined adversary. *See, e.g.*, King, *supra* note 141 ("The defenders have to be good everywhere; the attacker only has to

has no boundaries,[474] and has no legal obstacles with which to contend.[475] When confronted with sophisticated cyberdefenses, determined adversaries can redouble their efforts to exploit and target vulnerabilities or circumvent the target's cyberdefenses altogether using relatively unsophisticated social engineering-based attacks, such as those used to successfully penetrate RSA Security.[476] Additional defensive measures may bring no additional protection in real terms (i.e., companies still may be vulnerable), so it is not surprising to learn that companies weighing the cost of additional cybersecurity measures against the costs of not taking such measures frequently decide not to act.

For all of these reasons, corporate executives are understandably skeptical regarding the return on investment from dollars spent on vulnerability mitigation and have difficulty seeing the business case for increased cybersecurity resource expenditures. Section VII discusses a number of ways in which corporations can begin successfully to address the daunting cybersecurity challenges they face.

VII. PRIVATE SECTOR OPPORTUNITIES

A. Pathways to Effective Vulnerability Mitigation

As the U.S. private sector strives to bolster cybersecurity, due consideration should be given to: (1) basic cyberhygiene to protect against opportunistic cyberintrusions; (2) improved situational awareness through

---

be good on one place."). Consider the challenges involved in successfully securing a complex and interconnected system such as the smartgrid—our nation's next generation electric grid—or the current electric grid, where security has been "bolted on" because it was not originally "designed in." *Cf.* MITRE CORP., STANDARDIZING CYBER THREAT INTELLIGENCE INFORMATION WITH THE STRUCTURED THREAT INFORMATION EXPRESSION (STIX™) 3 (2012), http://makingsecuritymeasurable.mitre.org/docs/STIX-Whitepaper.pdf (considering how "intelligence-driven" computer network defense could potentially challenge the "conventional wisdom" that offense has an inherent advantage over defense and discussing potential opportunities to "fundamentally affect the balance of power between the defender and the adversary").

472. The cyberthreat against which companies are defending is constantly evolving with the result that "[e]ven big companies with significant IT staffs have difficulty keeping up with all the changes, updates, modifications, and upgrades necessary to keep up with the world of criminal hacking." Sherman, *supra* note 450.

473. SANS INST., AN UNEVEN PLAYING FIELD: THE ADVANTAGES OF THE CYBER CRIMINAL VS. LAW ENFORCEMENT—AND SOME PRACTICAL SUGGESTIONS 3–5 (2002), http://www.sans.org/reading_room/whitepapers/legal/uneven-playing-field-advantages-cyber-criminal-vs-law-enforcement-and-practica_115.

474. *Id.* at 7.

475. *Id.*

476. Bright, *supra* note 86 (calling the attack on RSA "run-of-the-mill" and explaining that it was not "extremely sophisticated" as originally suggested by RSA).

threat intelligence; and (3) adoption of cyberinsurance to manage the consequences of inevitable cyberintrusions.

1. Cyberhygiene

Many cybersecurity experts believe that basic cyberhygiene is a simple and logical first step in corporate cybersecurity.[477] Estimates suggest that good cyberhygiene could prevent up to eighty-five percent of cyber-intrusions, according to Howard Schmidt, former cybersecurity coordinator for President Obama.[478] Rather than waiting for legislative mandates or a cyberincident to spur corporate cybersecurity spending, corporations would be wise to consider whether some proactive investments in basic cyber-hygiene[479] are warranted as part of their basic corporate responsibility.[480] However, some argue that even basic cyberhygiene is expensive, if not cost-prohibitive, for some companies. A recent study lends some credence to that claim. Based on interviews with technology managers from 172 U.S. organizations in six industries, the study found that "[t]o be able to thwart 84 percent of attacks, up from the current 69 percent, respondents said they would have to almost double their average expenditures on

477. *A Brief History of the 20 Critical Security Controls*, SANS INST., http://www.sans.org/critical-security-controls/history.php (last visited Apr. 2, 2013) ("[T]he Commander of the US Cyber Command and Director of NSA announced that he believed adoption of the 20 Critical Controls was a good foundation for effective cybersecurity.").

478. *See* Howard Schmidt, *Price of Inaction Will Be Onerous*, N.Y. TIMES (Oct. 18, 2012), http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/price-of-inaction-on-cybersecurity-will-be-the-greatest ("It is estimated that as high as 85% of successful intrusions could have been prevented by just implementing good 'cyber-hygiene.' "); *see also* Press Release, Mac Thornberry, U.S. Representative, Cybersecurity Task Force Releases Recommendations (Oct. 5, 2011), *available at* http://thornberry.house.gov/news/documentsingle.aspx ?DocumentID=263044 ("The consensus among experts is that 85% of current cyberthreats can be thwarted by current cyber hygiene."). According to the Australian Department of Defence, "[a]t least 85% of the targeted [cyberintrusions] that the Defence Signals Directorate (DSD) responded to in 2010 could have been prevented by following the first four mitigation strategies listed in DSD's Top 35 Mitigation Strategies." *Strategies to Mitigate Targeted Cyber Intrusions*, AUSTRALIA DEP'T OF DEF.—DEF. SIGNALS DIRECTORATE, http://www.dsd.gov.au/infosec /top35mitigationstrategies.htm (last visited Apr. 2, 2013) (describing the top four mitigation strategies as: patching applications, such as Java and Microsoft Office; patching operating system vulnerabilities; minimizing the number of users of with administrative privileges; and application "whitelisting" which allows users to run only approved applications).

479. *See* John Brennan, *Cybersecurity Awareness Month Part III*, WHITE HOUSE BLOG (Oct. 19, 2009, 4:39 PM), http://www.whitehouse.gov/blog/Cybersecurity-Awareness-Month-Part-III (providing "tips" for improved cyber hygiene).

480. Ann Goodman, *Digital Security: Business's Social Responsibility*, ANN GOODMAN'S BLOG (July 1, 2012), http://anngoodman.com/2012/07/01/digital-security-a-business-social-responsibility/.

equipment and practices such as user verification systems, encryption and workforce training."[481]

2. Situational Awareness Through Threat Intelligence

Improving our nation's cybersecurity requires companies not just to invest *more* in cybersecurity, but to invest *wisely*. Today, many companies invest their cybersecurity dollars in intrusion detection systems and other perimeter defense systems designed to detect breaches. Cybersecurity experts have begun to challenge the "breach prevention" model of cybersecurity. For example, one expert writes:

> [W]e stubbornly adhere to Einstein's definition of insanity: doing the same thing over and over again and expecting a different outcome. In this case, that same thing is responding to breaches by investing disproportionate sums of money in perimeter defenses in a futile attempt to prevent breaches.
>
> . . . .
>
> Stop pretending you can prevent a perimeter breach. Accept that it will happen and build your security strategy accordingly. We need to admit that we, as an industry, have a problem. Start by asking yourself if your security philosophy has changed much in the last 10 years. It almost certainly has not. You're likely to be spending 90% of your security budget the same way you did back in 2002, which undoubtedly focuses on perimeter and network defenses.[482]

Perimeter defense systems do not tell you who is on your system, so once an adversary penetrates the network without being detected,[483] he may lurk undetected for years, as was the case with Operation Shady RAT.[484] Better situational awareness of corporate networks through threat intelligence is just one example of the ways in which corporations

---

481. Eric Engleman & Chris Strohm, *Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps*, BLOOMBERG (Jan. 31, 2012, 12:00 AM), http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html.

482. Tsion Gonen, *Breach Prevention is Dead. Long Live the 'Secure Breach,'* NETWORK WORLD (Oct. 29, 2012, 5:21 PM), http://www.networkworld.com/news/tech/2012/102912-secure-breach-263779.html.

483. Joseph Menn, *Hacked Firms Fight Back with Vigilante Justice*, GLOBE & MAIL (June 18, 2012, 1:58 PM), http://www.theglobeandmail.com/technology/tech-news/hacked-firms-fight-back-with-vigilante-justice/article4321501/ ("Consumer-grade antivirus you buy from the store does not work too well trying to detect stuff created by the nation-states with nation-state budgets.").

484. *See generally* ALPEROVITCH, *supra* note 96; Larry Greenemeier, *No Hacktivism Here: McAfee Reveals Cyber Espionage That Went Undetected for Years*, SCI. AM. (Aug. 3, 2011), http://blogs.scientificamerican.com/observations/2011/08/03/no-hactivism-here-mcafee-reveals-cyber-espionage-that-went-undetected-for-years/.

vulnerable to cyberespionage threats may be able to ramp up their cyberprotections.

For companies handling sensitive customer information, encryption is another relatively simple security measure to be considered.[485] Online retailer Zappos recently suffered a breach in which the attacker accessed customer information, but it is believed that the attackers received "virtually nothing of value from the theft" because the data was encrypted.[486] Some have even noted that the intrusion could "well make Zappos more secure moving forward, since potential attackers will know the company represents a poor investment of their time and effort."[487]

3. Insurance

Cybersecurity is much more than just a technical challenge. Recognizing that perfect security generally is unattainable, unnecessary, and cost-prohibitive,[488] most companies embrace risk management (i.e., managing the risk of loss due to cyberincidents) as a central element of information security.[489] The motivating principle behind the risk management approach to cybersecurity is to invest in security so as to reduce "expected losses" from attacks.[490] Such losses may include

485. Effective encryption implementations require, *inter alia*, successful key management and robust access controls. *See* VORMETRIC, DATA PROTECTION FOR PHYSICAL, VIRTUAL, AND CLOUD ENVIRONMENTS 1–2 (2012), http://www.vormetric.com/sites/default/files/sb-physical-virtual-cloud-environments-data-protection.pdf.

486. Gonen, *supra* note 482.

487. *Id.*

488. Kenneth L. Wainstein & Keith M. Gerver, *The Rockefeller Letter and the Cybersecurity Debate*, LEXOLOGY (Oct. 12, 2012), http://www.lexology.com/library/detail.aspx?g=a50ee1c0-2931-4550-9aaf-cc8da1dfe7c0 ("[O]ne recent survey of 172 U.S. companies found that they would have to boost their cyber spending almost 900% to achieve a level of security that would stop 95% of cyberattacks."); Engleman & Strohm, *supra* note 481 ("To achieve an ideal level of security in which 95 percent of attacks are thwarted, utilities and energy companies surveyed in the Bloomberg study would have to increase average annual spending more than seven-fold to $344.6 million per company from the current level of $45.8 million.").

489. In fact, critical infrastructure companies participating in a recent Bloomberg study said that they would need to nearly double their cybersecurity spending to improve the security of their systems, and even then would "remain vulnerable." Helen Domenici & Afzal Bari, *BGOV Study: The Price of Cybersecurity: Big Investments, Small Improvements*, BLOOMBERG GOV'T BLOG (Feb. 1, 2012), http://about.bgov.com/2012/02/01/bgov-study-the-price-of-cybersecurity-big-investments-small-improvements/; *see* ALPEROVITCH, *supra* note 96, at 6 (discussing how the availability of countermeasures against the bad actor "caused the perpetrator to adapt and increasingly employ a new set of implant families and [Command & Control] infrastructure").

490. Mulligan & Schneider, *supra* note 448, at 6.

reputational risk;[491] potential loss of valuable intellectual property; regulatory risk (e.g., regulatory penalties imposed for cybersecurity failure or failure to satisfy data breach notification requirements); and liability for loss due to negligence (e.g., liability for harm to consumers arising out of penetration of inadequately secured corporate networks).

Cyberinsurance is an important private sector risk-management tool. Over the past decade, the insurance industry's response to cyberrisks has evolved significantly. Initially, many standard policies were worded broadly enough to cover losses arising out of cybersecurity breaches; however, insurance companies quickly recognized this and moved to exclude cyberrisks from their standard coverage. To fill the resulting gap in coverage, insurers began marketing specialized cyberinsurance policies.[492]

Cyberinsurance has a number of important benefits. Specifically,

> Cyber-insurance increases cyber-security by encouraging the adoption of best practices. Insurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security. The security requirements used by cyber-insurers are also helpful. With widespread take-up of insurance, these requirements become de facto standards, while still being quick to update as necessary. Since insurers will be required to pay out cyber-losses, they have a strong interest in greater security, and their requirements are continually increasing. [493]

Accordingly, a well-functioning cyberinsurance market could help to "align private incentives with the overall public good."[494]

Despite the potential benefits of cyberinsurance, the industry has been slow to purchase policies, with only about thirty-five percent of public companies currently investing in such coverage.[495] In some cases,

---

491. Gorman & Tibken, *supra* note 162 (noting that despite mitigation measures, a security breach will still hurt RSA's reputation).

492. Louis Chiafullo & Brett Kahn, *Coverage for Cyber Risks*, COVERAGE, ABA SECTION ON LITIG., COMMITTEE ON INS. COVERAGE LITIG., May/June 2011, at 3, 7, http://www.meagher.com/files/upload /Coverage_MayJune2011_Woodworth.pdf.

493. WHITE HOUSE, CYBER-INSURANCE METRICS AND IMPACT ON CYBER-SECURITY 1–2, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf.

494. Walter S. Baer & Andrew Parkinson, *Cyberinsurance in IT Security Management*, IEEE SECURITY & PRIVACY 50 (2007), http://www.sis.pitt.edu /~dtipper/2825/CIn.pdf.

495. *See Chubb 2012 Public Company Risk Survey: Cyber—Did You Know?*,

executives may not think that their companies are vulnerable to attack, and, in other cases, cyberinsurance simply may be cost-prohibitive.[496]

2013 may be the year of cyberinsurance as executives (1) come to better understand the threats of cybercrime, cyberespionage, and cyberwar; and (2) deal with legal and regulatory developments, including the SEC's game-changing cybersecurity guidance issued in October of 2011.[497] This staff-level guidance not only clarifies that companies must report "material information regarding cybersecurity risks and cyber incidents," but also provides that "to the extent material, appropriate disclosures may include . . . [d]escription of relevant insurance coverage."[498] The SEC's staff guidance is expected to spur corporate interest in cyberinsurance,[499] as would the more formal SEC guidance Senator Rockefeller has urged the SEC to adopt.[500]

Some foresee a system in which (1) civil liability is imposed for cybersecurity breaches (possibly with safe harbors or other limitations on

---

CHUBB GRP. OF INS. COS., http://www.chubb.com/infographics/chubb3/index.html (last visited Apr. 2, 2013); *see also* Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. TIMES BITS BLOG (Dec. 29, 2011, 10:50 AM), http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/ ("[O]nly a third of companies surveyed by Advisen, a research group, say they have purchased a cyber insurance policy.").

496. Specialized cybercoverage is expensive for a number of reasons. First, considerable uncertainty remains about the appropriate pricing of cyberinsurance policies. While insurers are aware of the risk of very large losses, they lack the empirical data necessary to construct actuarial tables (in part this is true because systems—and hence vulnerabilities—change quickly such that "the past is not a good predictor of the future"). Second, networked information systems are particularly vulnerable to a major disaster that could result in a large number of claims. Accordingly, the cost of re-insurance for cyberinsurers is high. Finally, barriers to entry into the cyberinsurance market reduce competition. One significant barrier to entry is that a catastrophic event could occur before an insurer has "built up sufficient cash reserves" to pay out on its policies. CYBER-INSURANCE METRICS AND IMPACT ON CYBER-SECURITY, *supra* note 493; Press Release, Eur. Network Info. Sec. Agreement, ENISA Report Calls for Kick-Start in Cyber Insurance Market (June 29, 2012), *available at* http://www.enisa.europa.eu/media/press-releases/enisa-report-calls-for-kick-start-for-kick-start-in-cyber-insurance-market ("[To date,] obstacles to the development of an effective cyber insurance market have included lack of actuarial data on the extent of the risk and uncertainty about what type of risk should be insured against.").

497. *CF Disclosure Guidance*, *supra* note 288.

498. *Id.*

499. *See* Perlroth, *supra* 495 (reporting an insurance broker's prediction that cyberinsurance premiums could grow by fifty percent in the twelve to eighteen month period starting in January 2012).

500. Elizabeth Wasserman, *SEC Urged to Give Stronger Guidance on Cyber Disclosure*, BLOOMBERG, (Apr. 10, 2013, 9:57 AM), http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html.

cybersecurity liability where industry has made a reasonable effort to conform to insurer-adopted best practices); (2) private insurers cover industry losses; and (3) the government offers backstop reinsurance for cyberinsurers to help reduce the price of cyberinsurance, thereby improving private sector access to cyberinsurance, and, arguably, leading to improved cybersecurity.[501]

Others have suggested that the federal government use its market power to promote cyberinsurance by requiring its contractors and subcontractors to carry cyberinsurance.[502] This approach would directly increase demand for cyberinsurance. Moreover, companies that purchase cyberinsurance to meet federal contracting requirements presumably would tout their coverage as a competitive advantage when bidding on private contracts, thereby putting pressure on their competitors to purchase cyberinsurance. Accordingly, some argue that this approach would ultimately bring about improved security, more insured companies, and, potentially, reduced costs for insurance coverage.[503] To the extent that development of an insurance market leads to improved security, one might view insurance as part of a holistic vulnerability mitigation strategy, but, at the end of the day, insurance largely is a form of consequence management—a means by which companies manage the consequences of cyberintrusions—and will not, by itself, stop cyberintrusion.

Basic hygiene, improved situational awareness, and maturation of the cyberinsurance market all contribute to vulnerability mitigation, yet vulnerability mitigation alone will not solve the U.S. cybersecurity problem.

B. Beyond Vulnerability Mitigation

The prevailing approach to cybersecurity in the U.S. has been vulnerability mitigation, but the rapid emergence of cyberespionage and cyberattacks as long-term threats to U.S. economic and national security necessitates a serious reevaluation of the private sector's role in cybersecurity as well as U.S. cybersecurity policy. Determined adversaries will find a way to successfully breach even the most sophisticated and heavily fortified organizations, as demonstrated by the successful attacks on DoD, RSA, Lockheed Martin, and Google. Simply throwing money at the cybersecurity problem and attempting to build higher fences around important corporate networks is not proving itself to be a workable long-term solution for U.S. industry, as the above-mentioned Bloomberg study

501. CYBER-INSURANCE METRICS AND IMPACT ON CYBER-SECURITY, *supra* note 493, at 4–5.

502. *Id.* at 3.

503. *Id.* at 5.

suggests.[504] Nor can corporations afford to rely solely on law enforcement efforts to track down and bring perpetrators to justice, as law enforcement is "overwhelmed" by the problem,[505] and hindered by a host of jurisdictional and other issues.[506]

The private sector should give serious consideration to potential options for threat deterrence. As the private sector shifts from a "perimeter defense" to a "threat intelligence" model, it simultaneously should explore the feasibility of "active defense"[507] and other innovative approaches to cybersecurity threats. The spectrum of "active defense"[508] ranges from "modest steps to distract and delay a hacker"[509] to more controversial

---

504. Engleman & Strohm, *supra* note 481.

505. Stewart Baker et al., *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ ("Cybercrime has cost consumers and banks billions of dollars. Yet few cyberspies or cybercriminals have been caught and punished. Law enforcement is overwhelmed both by the number of attacks and by the technical unfamiliarity of the crimes."); Tim Wilson, *Companies Should Think About Hacking Back Legally, Attorney Says*, DARK READING (Nov. 1, 2012, 7:45 AM), http://www.darkreading.com/risk-management/167901115/security/security-management/240012675/companies-should-think-about-hacking-back-legally-attorney-says.html ("Calling law enforcement doesn't help—they are simply overwhelmed with other cases."); Ellen Nakashima, *Several Nations Trying to Penetrate U.S. Cyber-Networks, Says Ex-FBI Official*, WASH. POST (Apr. 18, 2012), http://articles.washingtonpost.com/2012-04-18/world/35451842_1_cyber-private-sector-networks (" 'I know a lot of companies have suffered, and they are going to want to see somebody come in and assist them,' said [Shawn] Henry, former executive assistant director of the FBI's Criminal, Cyber, Response and Services Branch. 'It won't be the U.S. government . . . . so it's going to have to be the private sector.' ").

506. SANS INST., *supra* note 473, at 7–8.

507. The concept of "active defense" stands in contrast to "passive defense" which relies on firewalls, patches, and anti-virus software. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 417, 461 (2012) ("Active defenses are a . . . category of response to cyberattacks and enable attacked parties to detect, trace, and then actively respond to a threat by, for example, interrupting an attack in progress to mitigate damage to the system.").

508. *Id.* at 513 (asserting that active defense is not a unitary whole and describing the different aspects of active defense as "detecting, tracing and [mitigative or retributive] counterstriking").

509. The military has been interested in "active defense" for years. *See, e.g.*, John Stanton, *Rules of Cyber War Baffle U.S. Government Agencies*, NAT'L DEF. MAG. (Feb. 2000), http://www.nationaldefensemagazine.org/archive/2000/February/Pages/Rules4391.aspx ("The Air Force Research Lab . . . has in place a number of cyber-defense mechanisms such as false databases made from deception software (available on the Internet) that create a bogus trail for potential hackers."). A TransAttack—or forensic analysis—begins once an attack is detected. As described by an Air Force Research Lab employee, "While the attack is happening we gather the evidence: Who is doing this? Where are they?" *Id.* Today, private sector security companies offer "active defense" approaches, including deception, to their clients. Liam Tung, *CrowdStrike Boss Explains Offensive Security in Targeted Attacks*, CSO (Aug. 9, 2012,

measures,[510] the legality of some of which may be unclear under today's laws. Some examples of active defense include:

> First, installing honeypots, fake networks and fake documents to slow the attackers down, leave them confused, and perhaps provide the defenders an early warning that the outer walls have been breached. Second, building 'beacons' into your documents, so when they're stolen and opened by the attackers, the documents phone home, telling you not only that you've been compromised, but [also] maybe something about the guys who did it.[511]

Finally, the private sector should consider how to change the .com cybersecurity debate in Washington, which has long-focused on vulnerability mitigation. For political and other reasons, today's debate remains focused on information sharing and voluntary standards, which, according to some experts, may be helpful only "in the margins."[512] The

---

11:44 AM), http://www.cso.com.au/article/433128/crowdstrike_boss_explains_offensive_security_targeted_attacks/ ("[Companies are increasingly demanding] deception, denial, disruption. They're moving more into the government mindset of deception. [Imagine, hypothetically, that] somebody breaks in and steals the plans [for Norththrop Grumman's B-2 Stealth Bomber.] [B]ut if the plans are wrong and the thing doesn't fly, think about the cost of that [to the adversary].").

510. "Hackback" is at the more aggressive end of the "active defense" spectrum, and an animated debate is raging among the cyber-elite over its legality as well as its advisability as a matter of policy. *See* Stewart Baker, *RATs and Poison: Can Cyberespionage Victims Counterhack?*, SKATING ON STILTS (Oct. 13, 2012), http://www.skatingonstilts.com/skating-on-stilts/2012/10/us-law-keeps-victims-from-counterhacking-intruders.html (making a policy case for counterhacking); Stewart Baker, *RATs and Poison II – The Legal Case for Counterhacking*, VOLOKH CONSPIRACY (Oct. 14, 2012, 2:51 pm), http://www.volokh.com/2012/10/14/rats-and-poison-ii-the-legal-case-for-counterhacking/ (making the legal case for counterhacking); Baker et al., *supra* note 505 (debating on legal and policy grounds the following questions: "Can the victims of hacking take more action to protect themselves? Can they hack back and mete out their own justice?"); *see also* Patrick Lin, *'Stand Your Cyberground' Law: A Novel Proposal for Digital Security*, THE ATLANTIC (Apr. 30, 2012, 12:59 PM) http://www.theatlantic.com/technology/archive/2012/04/stand-your-cyberground-law-a-novel-proposal-for-digital-security/256532/; Taylor Armerding, *Should Best Cybercrime Defense Include Some Offense?*, NETWORK WORLD (June 20, 2012, 7:50 AM), http://www.networkworld.com/research/2012/061912-should-best-cybercrime-defense-include-260345.html; Wilson, *supra* note 505 ("Hacking back should never be a company's first response, but in the case of a persistent attacker, it might be the only answer. 'You might be spending $50,000 to $100,000 a week to battle a persistent threat' [attorney David Willson] says. 'You've tried all of the traditional approaches.' ").

511. Stewart Baker, *Taking the Offense to Defend Networks,* STEPTOE CYBERBLOG (June 19, 2012), http://www.steptoecyberblog.com/2012/06/19/taking-the-offense-to-defend-networks/; *see* Wilson, *supra* note 505.

512. Ellen Nakashima, *Cybersecurity Should Be More Active, Official Says*, WASH. POST (Sept. 16, 2012), http://articles.washingtonpost.com/2012-09-16/world/35494752_1_top-cyber-private-sector-crowdstrike (quoting Steven Chabinsky, former Deputy Assistant Director of the FBI's Cyber Division and current

private sector should urge Congress to broaden the debate to include consideration of the private sector's potentially game-changing role in threat deterrence. The private sector should urge Congress to remove barriers to private sector efforts to develop innovative approaches to threat deterrence. The private sector simultaneously should urge the government to bring all elements of national power—including economic,[513] diplomatic,[514] and military[515]—to bear to deter would-be threat actors.

Senior Vice President of Legal Affairs and Chief Risk Officer at CrowdStrike).

513. On the economic front, the private sector could, for example, press for greater domestic legal protections from the threat of economic espionage, potentially including penalties for those Chinese companies benefitting from industrial espionage. This would be a natural extension of the U.S.-China Economic and Security Review Commission recommendations that Congress "conduct a review of existing legal penalties for companies found to engage in, or benefit from, industrial espionage." U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 186, at 188; *see* Gerald O'Hara, Comment, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 244 (2010) (discussing the Economic Espionage Act and concluding that "current law is inadequate to deal with the cybertheft of corporate trade secrets"). Others have suggested that the United States use the Committee on Foreign Investment in the United States ("CFIUS") approval process for leverage. *See* Stewart Baker, *More on Cybersecurity and Attribution: Si Chuan University and Tencent*, STEPTOE CYBERBLOG (Dec. 5, 2012), http://www.steptoecyberblog.com/2012/12/05/more-on-cybersecurity-and-attribution-si-chuan-university-and-tecent/. CFIUS is the "inter-agency committee authorized to review transactions that could result in control of a U.S. business by a foreign person . . . in order to determine the effect of such transactions on the national security of the United States." *See Committee on Foreign Investment in the United States (CFIUS)*, U.S. DEP'T OF THE TREAS. RES. CTR., http://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx (last updated Dec. 20, 2012, 1:37 PM).

514. The administration recently stepped up efforts to address the threat of Chinese cyberespionage through diplomatic channels, beginning with National Security Advisor Tom Donilon's speech at the Asia Society. Donilon, *supra* note 213 ("Specifically with respect to the issue of cyber-enabled theft, we seek three things from the Chinese side. First, we need a recognition of the urgency and scope of this problem and the risk it poses—to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace . . . ."). *See also infra* Section IV.B.5. However, much work remains to be done. On the diplomatic front, the United States can act through a variety of channels, potentially including the WTO, to penalize companies that benefit from industrial espionage and to "discourage foreign countries from enabling or tolerating cyberespionage." O'Hara, *supra* note 513, at 274 ("[T]he President should instruct the United States Trade Representative to engage strategic allies to coauthor a resolution decrying the use of cyber attacks to misappropriate proprietary economic information. There are many countries in both the developed and developing blocs that have much to lose through cyber-espionage attacks, and using the WTO as a vehicle to navigate change on intellectual property protection has been successful in the past.").

515. The United States needs to continue to develop its military strategy for deterring cyberattacks. General Alexander's public testimony on March 12, 2013 clearly plays into such a strategy by identifying the capabilities CyberCom is

With these actions, it is hoped that the fiddlers on the roof will "[keep their] balance . . . for many, many years"[516] to come.

developing and how they are to be used. Specifically General Alexander told Congress that he is developing "an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace" and that "[t]hirteen of the teams that [the Pentagon is] creating are for that mission alone." Mazzetti & Sanger, *supra* note 223; Richard Lardner, *Pentagon Forming Cyber Team to Prevent Attacks*, PHYS.ORG (March 12, 2013), http://phys.org/news/2013-03-deters-major-cyberattacks.html#jCp ("Alexander told the Senate Armed Services Committee that foreign leaders are deterred from launching cyberattacks on the United States because they know such a strike could be traced to its source and would generate a robust response."). Alexander's comments certainly appear to have been designed to serve a deterrence function. *See generally* Jack Goldsmith, *The Significance of Panetta's Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks*, LAWFARE (Oct. 15, 2012, 1:26 PM), http://www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks/ (discussing then-Defense Secretary Panetta's speech and suggesting that "the speech's real significance . . . concerns DOD's evolving deterrence posture . . . . Panetta had two main messages related to deterrence. [First,] '[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.' Second, . . . he makes plain that the DOD has the capabilities and desire to engage in a *preemptive* attack[] against *imminent* cyber threats.") (emphasis in original). *See* Charles L. Glaser, *Deterrence of Cyber Attacks and U.S. National Security*, GEO. WASH. UNIV. CYBER SECURITY POL'Y AND RES. INST. 6 (2011) http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf ("Deterring cyber attacks may not be as difficult as the emerging conventional wisdom suggests. . . . To support its deterrence policy, the United States needs a clear declaratory policy that lays out its plans for responding to various types of attacks.").

516. FIDDLER ON THE ROOF, *supra* note 1.