Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate[*]

> *"If you spend more on coffee than on IT security, then you will be hacked. . . . What's more, you deserve to be hacked."*[1]

I. Introduction

On January 28, 2011, Egypt vanished—not literally, but digitally. Following massive demonstrations against Egyptian President Hosni Mubarak's regime,[2] the Egyptian government shut off Internet access across the country, a move "unprecedented in Internet history."[3] With access to social-networking sites cut off, even more citizens stormed the streets of Cairo, adding Internet connectivity to their list of political demands and transforming Tahrir Square into a "street Twitter."[4]

Though the logistics of Egypt's "Internet kill switch" remain foggy,[5] the event has set the stage for a serious debate about cybersecurity issues within the United States, including whether or not the United States government should be given access to a kill switch of its own.[6] A series of high-profile Internet attacks in the last two years underscores the severity of the problem.[7]

[*] Thank you to my friends—the members of the *Texas Law Review*—for their help preparing this Note for publication. Thanks also to Andrew C. Payne for the initial inspiration that evolved into this piece. Any errors remain my own.

[1] Robert Lemos, *Security Czar: Button Up or Get Hacked*, CNET NEWS (Feb. 19, 2002), http://news.cnet.com/2100-1001-840335.html (quoting Richard Clarke, Special Adviser on Cybersecurity to President George W. Bush).

[2] *See generally* Kareem Fahim & Mona El-Naggar, *Violent Clashes Mark Protests Against Mubarak's Rule*, N.Y. TIMES, Jan. 25, 2011, *available at* http://www.nytimes.com/2011/01/26/world/middleeast/26egypt.html.

[3] James Cowie, *Egypt Leaves the Internet*, RENESYS BLOG (Jan. 27, 2011, 7:56 PM), http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml; *see also* Noam Cohen, *Egyptians Were Unplugged, and Uncowed*, N.Y. TIMES, Feb. 20, 2011, *available at* http://www.nytimes.com/2011/02/21/business/media/21link.html (labeling January 28 "the day the Internet died").

[4] Cohen, *supra* note 3. Protesters displaying signs reading "I want Internet" were visible days into the digital blackout. *Id.*

[5] *Compare* Ryan Singel, *Report: Egypt Shut Down Net with Big Switch, Not Phone Calls*, WIRED (Feb. 10, 2011), http://www.wired.com/threatlevel/2011/02/egypt-off-switch/ (alleging that a breaker in the "Internet Exchange Point" known as the "Ramses exchange" was flipped), *with* Cowie, *supra* note 3 (modeling the blackout and concluding that Internet service providers were likely told individually to "take themselves off the air").

[6] *See, e.g.*, Chloe Albanesius, *Lieberman Backs Away From "Internet Kill Switch,"* PC MAG (June 21, 2010), http://www.pcmag.com/article2/0,2817,2365393,00.asp (reporting that Senator Joseph Lieberman has recently advocated granting the government the power to "disconnect parts of its Internet in a case of war").

[7] *See infra* Part III.

The dizzying array of approaches to the issue illustrates the need for clarity and uniformity.[8]

This Note proceeds in five parts. Part II lays a foundation by tracing the history of the Internet and, with it, the creation of innumerable computer security threats, from the simple virus to complex, system-specific worms. In Part III, a handful of stories demonstrate the vulnerability of Internet-connected networks and much of America's critical infrastructure. Part IV reviews the various proposals, both on and off the books, to cope with the cybersecurity problem. Drawing upon those and other ideas, Part V offers an initial framework for protecting the Internet. Part VI briefly concludes.

II. Historical Background

A. *The Rise of the Internet*

The history of the Internet begins with a satellite. President Dwight Eisenhower, in response to the launch of the Russian satellite Sputnik in 1958, created the Advanced Research Projects Agency (ARPA)[9] to develop technologies for use by America's military.[10] Initial projects focused on traditional military systems like missile defense, but by 1962, ARPA's Information Processing Techniques Office had begun to drive the field of computer science forward.[11] ARPA's goal was to bring together researchers from across the country via a computer network humbly named ARPANET.[12] The potential military uses of such a network were quickly realized by ARPA's tech gurus.[13]

The single-network ARPANET was transformed into the multi-network Internet over the next ten years.[14] As ARPANET's user base grew (limited primarily to Department of Defense officials and contractors), its users began to realize the usefulness of features like electronic mail.[15] Simultaneously, the American military was busily introducing computer technology in myriad ways, which required ARPA to expand the network in a way that

[8] *See infra* Part IV.

[9] Pub. L. No. 85-325, 72 Stat. 11 (1958). In its relatively short history, ARPA's official name has fluctuated between ARPA and DARPA (adding or removing "Defense") multiple times. *ARPA-DARPA: The Name Chronicles*, DEF. ADVANCED RESEARCH PROJECTS AGENCY, http://www.darpa.mil/About/History/ARPA-DARPA__The_Name_Chronicles.aspx. For consistency, this Note uses ARPA exclusively.

[10] JANET ABBATE, INVENTING THE INTERNET 36 (1999); *see also* ROBERT J. WATSON, INTO THE MISSILE AGE, 1956–1960, at 187–91 (1997) (describing the creation of ARPA).

[11] ABBATE, *supra* note 10, at 36.

[12] *Id.* at 37.

[13] ARTHUR L. NORBURG ET AL., TRANSFORMING COMPUTER TECHNOLOGY: INFORMATION PROCESSING FOR THE PENTAGON, 1962–1986, at 172 (1996).

[14] ABBATE, *supra* note 10, at 113. *See generally* Mitch Waldrop, *DARPA and the Internet Revolution*, *in* DARPA: 50 YEARS OF BRIDGING THE GAP 78, 78–85 (2008) (chronicling ARPA's involvement in the creation of the Internet).

[15] NORBURG ET AL., *supra* note 13, at 178.

incorporated those different systems.[16] Ultimately, the diverging needs of ARPA's research users and its military users forced the Department of Defense to bifurcate the network: ARPANET would provide an experimental platform for defense researchers, while MILNET would provide a stable, restricted-access network for military communications.[17] Coincidentally, separating the operational military components also made it easier for ARPANET to be commercialized and emerge as the Internet of today.[18]

Commercialization and privatization of the Internet resulted in rapid expansion. In 1998, the Department of Commerce was still defining "the Internet" in its economic reports.[19] Commerce attributed the Internet's tremendous growth to "its strength as a medium of communication, education and entertainment, and . . . as a tool for electronic commerce."[20] By 2010, the need to define the ubiquitous network was wholly unnecessary: roughly two billion people were Internet users, double the number of users connected just five years earlier.[21]

The Internet continues to spread hand-in-hand with new tools for connecting and reconnecting with others. Increasingly popular social-networking sites[22]—reflections of the Internet's communal legacy—illustrate the degree to which network-based communication has been incorporated into the social consciousness.[23] But as the number of network-connected

[16] ABBATE, *supra* note 10, at 124.

[17] *Id.* at 142–43; NORBURG ET AL., *supra* note 13, at 185.

[18] ABBATE, *supra* note 10, at 143. ARPA officially relinquished control over the Internet in the 1980s, when its expansion and growth quickened:

> At the beginning of the 1980s, the Internet included only a relatively small set of networks, most of which had direct links to defense research or operations. Over the course of the 1980s and the 1990s, the Internet would grow enormously in the number of networks, computers, and users it included; it would be transferred from military to civilian control; and its operation would be privatized, making the network much more accessible to the general public.

Id. at 181.

[19] U.S. DEP'T OF COMMERCE, THE EMERGING DIGITAL ECONOMY 1 n.* (1998), *available at* http://www.esa.doc.gov/sites/default/files/reports/documents/emergingdig_0.pdf.

[20] *Id.* at 1.

[21] *The World in 2010: ICT Facts and Figures*, INT'L TELECOMM. UNION (2010), *available at* http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[22] *See* Bill Tancer, *Facebook: More Popular than Porn*, TIME, Oct. 31, 2007, *available at* http://www.time.com/time/business/article/0,8599,1678586,00.html (indicating that social-networking sites are the most visited category of websites among users between the ages of 18 and 24).

[23] *See* Ann E. O'Connor, Note, *Access to Media All A-Twitter: Revisiting* Gertz *and the Access to Media Test in the Age of Social Networking*, 63 FED. COMM. L.J. 507, 528 n.117 (2010) (chronicling the role of social-networking sites in recent political uprisings in Tunisia and Egypt); *see also* Seth F. Kreimer, *Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet*, 150 U. PA. L. REV. 119, 170 (2001) ("The Internet is in the process of being incorporated into American social movements' repertoires of collective action.").

users rises, so too does the number of potential targets and the avenues available to users with malicious intent.[24]

B. The Rise of the Computer Virus (and Other Unsavory Characters)

Despite its military roots, the Internet's architects deny the popular mythos that the network was ever designed to be secure.[25] The explosive growth of the information superhighway resulted in a sprawling web of networks flush with security problems.[26] Interconnectedness meant that computer viruses, once contained to spreading via physical media like floppy disks, could be mobilized to spread over the emerging Internet.[27] The e-mail systems that early ARPANET users found so attractive became breeding grounds for viruses that propagated themselves via seemingly innocuous attachments.[28] As Internet-browsing software became more robust by allowing for common user actions to be automated, even more security vulnerabilities emerged.[29]

Today's Internet is a virtual smorgasbord of dangerous material. Computer users and network administrators must worry about backdoors,[30]

[24] *See, e.g.*, MCAFEE LABS, 2011 THREATS PREDICTIONS 4 (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2011.pdf ("Social media connections will eventually replace email as the primary vector for distributing malicious code and links. The massive amount of personal information online coupled with the lack of user knowledge of how to secure this data will make it far easier for cybercriminals to engage in identity theft and user profiling than ever before.").

[25] *See* John Carlin, *A Farewell to Arms*, WIRED, May 1997, *available at* http://www.wired.com/wired/archive/5.05/netizen.html ("The Internet, [Howard Frank, Director of DARPA's Information Technology Office] says, was never designed to survive a nuclear war. Claims that it was designed to be invulnerable are urban myth, he's happy to tell you."); *see also* CTR. FOR STRATEGIC & INT'L STUDIES, CYBERSECURITY TWO YEARS LATER 2 (2011) [hereinafter CSIS REPORT] ("The Internet was not designed to be a global infrastructure on which hundreds of millions of people would depend.").

[26] *See Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 111th Cong. 14 (2010) (statement of James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies) ("That technologies designed in the early 1970s have worked so well and have so cleanly scaled to support more than a billion users is an amazing triumph, but anyone with malicious intent can easily exploit these networks. The Internet was not designed to be a global infrastructure upon which hundreds of millions of people would depend. It was never designed to be secure. . . . [W]e must now recognize that this pioneer approach is now inadequate."); CSIS REPORT, *supra* note 25, at 7 ("The market will not deliver adequate security in a reasonable period, and voluntary efforts will be inadequate against advanced nation-state opponents.").

[27] DOUG HOWARD & KEVIN PRINCE, SECURITY 2020: REDUCE SECURITY RISKS THIS DECADE 3–4 (2011).

[28] *See* 1 THE INTERNET ENCYCLOPEDIA 254–55 (Hossein Bidgoli ed., 2004) (describing the proliferation of the early "Melissa" virus via *.doc e-mail attachments).

[29] DAVID KIM & MICHAEL G. SOLOMON, FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY 361–62 (2012).

[30] A backdoor is "[a]n undocumented and often unauthorized access method to a computer resource that bypasses normal access controls." *Id.* at 478.

botnets,[31] denial-of-service attacks,[32] keyloggers,[33] logic bombs,[34] malware,[35] pharming,[36] phishing,[37] rootkits,[38] smurfing,[39] spoofing,[40] spyware,[41] Trojan horses,[42] viruses,[43] worms,[44] and more.

Against this backdrop of potential hazards, it is no surprise that the media has long sensationalized the cybersecurity issue.[45] It is also unsurprising that Congress has echoed the media's concerns, warning of a catastrophic future attack akin to a "cyber 9/11."[46] The White House has joined the fray

[31] "A botnet consists of a network of compromised computers [(bots)] that attackers use to launch attacks and spread malware." *Id.*

[32] A denial of service (DoS) attack "uses ping or ICMP echo-request, echo-reply messages to bring down the availability of a server or system." *Id.* at 480.

[33] A keylogger is a program that "records to a log file every keystroke a user makes." *Id.* at 484.

[34] A logic bomb is "[a] program that executes a malicious function of some kind when it detects certain conditions." *Id.* at 485. "A logic bomb, when 'exploded,' may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects." THE INTERNET ENCYCLOPEDIA, *supra* note 28, at 334.

[35] Malware, "[s]hort for malicious software," is "designed to infiltrate one or more target computers and follow an attacker's instructions." KIM & SOLOMON, *supra* note 29, at 485.

[36] Pharming is a type of "attack that seeks to obtain personal or private financial information through domain spoofing." *Id.* at 486.

[37] Phishing is "[a] type of fraud in which an attacker attempts to trick the victim into providing private information." *Id.* at 487.

[38] "Rootkits in Windows refers to programs that use system hooking or modification to hide files, processes, registry keys, and other objects in order to hide programs and behaviors." SYMANTEC, WINDOWS ROOTKIT OVERVIEW 4 (2005), *available at* http://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf.

[39] Smurfing is a type of DoS attack "that uses a directed broadcast to create a flood of network traffic for the victim computer." KIM & SOLOMON, *supra* note 29, at 489.

[40] Spoofing is a type of "attack in which one person, program, or computer disguises itself as another person, program, or computer to gain access to some resource." *Id.* at 490.

[41] Spyware is a class of "[s]oftware that gathers user information through the user's Internet connection without the user's knowledge." *Id.*

[42] A Trojan horse is "[a]n apparently innocuous program that contains code designed to surreptitiously access information or computer systems without the user's knowledge." THE INTERNET ENCYCLOPEDIA, *supra* note 28, at 335.

[43] A virus is "[a] computer program designed to replicate or copy itself and spread the copies . . . from one machine to another without the aid, and often without the knowledge, of the user." *Id.*

[44] "A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of a computer operating system that are automatic and usually invisible to the user." *Id.*

[45] *See, e.g.*, JUSSI PARIKKA, DIGITAL CONTAGIONS: A MEDIA ARCHAEOLOGY OF COMPUTER VIRUSES 93–95 (2007) (chronicling "the general virus hype or hysteria" present throughout the 1980s and 1990s).

[46] 157 CONG. REC. S912 (daily ed. Feb. 17, 2011) (statement of Sen. Collins); *see also id.* at S910 ("[T]he computer systems of Congress and the Executive Branch agencies are now under cyber attack an average of 1.8 billion times per month. The annual cost of cyber crime worldwide has climbed to more than $1 trillion. . . . Devastating cyber attacks could disrupt, damage, or even destroy some of our nation's critical infrastructure, such as the electric power grid, oil and gas pipelines, dams, or communications networks. These cyber threats could cause catastrophic damage in the physical world.").

as well, calling for action before a digital attack "cripple[s] society."[47] In some situations, the alarmist rhetoric has lost touch with reality, suggesting that nefarious hackers can take control of the Hoover Dam and open its floodgates at will, "kill[ing] thousands of people in the process."[48] Though such wild speculation is demonstrably false,[49] it nevertheless serves to create an atmosphere of danger and fear in an attempt to justify government restrictions. A sober analysis of several of the largest cybersecurity incidents in recent memory serves to illustrate the true scope of the risks the country faces in order to more accurately inform the debate about how to secure the Internet.

III. Modern Cybersecurity Threats

A. The SQL Slammer

Discussions of America's inadequately secured power grid often center around the 2003 "SQL Slammer" worm. At 12:30 a.m. (EST) on January 25, 2003, Slammer infected its first computer: a web server running Microsoft's database software SQL (commonly pronounced "sequel").[50] Slammer was designed to replicate itself and send new copies out across the Internet.[51] That simple but ruthlessly efficient design ensured that by 12:33 a.m., only minutes after Slammer claimed its first victim, the number of infected machines was doubling every 8.5 seconds.[52]

[47] EXEC. OFFICE OF THE PRESIDENT OF THE U.S., CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 2 (2009) [hereinafter CYBERSPACE POLICY REVIEW] ("The growing sophistication and breadth of criminal activity, along with the harm already caused by cyber incidents, highlight the potential for malicious activity in cyberspace to affect U.S. competitiveness, degrade privacy and civil liberties protections, undermine national security, or cause a general erosion of trust, or even cripple society.").

[48] David Kravets, *No, Hackers Can't Open Hoover Dam Floodgates*, WIRED (Feb. 3, 2011), http://www.wired.com/threatlevel/2011/02/hoover/. Hollywood-inspired ideas like this are not new. In 2001, *USA Today* offered a similar warning:

> [A]n adversary could use . . . viruses to launch a digital blitzkrieg against the United States. It might send a worm to shut down the electric grid in Chicago and air-traffic-control operations in Atlanta, a logic bomb to open the floodgates of the Hoover Dam and a sniffer to gain access to the funds-transfer networks of the Federal Reserve.

Andrea Stone, *Cyberspace: The Next Battlefield*, USA TODAY, June 19, 2001, *available at* http://www.usatoday.com/tech/news/2001-06-19-cyberwar-full.htm.

[49] The U.S. Bureau of Reclamation, which oversees operation of the Hoover Dam, has explicitly denied that such vulnerabilities are even possible:

> "I'd like to point out that this is not a factual example, because Hoover Dam and important facilities like it are not connected to the internet," Peter Soeth, a spokesman for the bureau, said in an e-mail. "These types of facilities are protected by multiple layers of security, including physical separation from the internet, that are in place because of multiple security mandates and good business practices."

Kravets, *supra* note 48.

[50] Paul Boutin, *Slammed!*, WIRED, July 2003, *available at* http://www.wired.com/wired/archive/11.07/slammer.html.

[51] *Id.*

[52] *Id.*

One infected network belonged to Ohio utility company FirstEnergy; it was located in their Davis-Besse nuclear power plant.[53] Slammer snaked its way into the plant's systems via a contractor's unsecured connection and began to slow down the plant's servers due to the constant flow of Slammer copies being flung out across the network.[54] Eventually, two monitoring systems at the plant crashed and were not restored until six hours had passed.[55]

Alarmists like Richard Clarke, a former Special Advisor on Cybersecurity to President George W. Bush, latched onto that incident as proof that hackers can compromise America's power grid at will. Clarke connected Slammer's infiltration of the Davis-Besse plant to a nearby regional power outage resulting from a fallen tree limb.[56] Although an alarm system within FirstEnergy's grid malfunctioned at the time of the blackout, causing it to spread farther than necessary, there was no demonstrable connection between the blackout, the alarm system, and Slammer.[57] Clarke's bold assertion that "the same effects could have been achieved by a command given over the control system by a hacker" was therefore unsupported.[58] That belief apparently had been buttressed by a vague statement from CIA expert Tom Donahue, who indicated that hackers had caused blackouts in other countries, presumably including a 2007 blackout in Brazil.[59] Yet Brazil's blackout had a much more plausible explanation, one supported by the numerous investigative efforts that probed deeper into the incident: high-voltage insulators clogged with soot from nearby burning fields, exacerbated by an eight-month drought.[60]

As Ralph Waldo Emerson once told a crowd of Phi Beta Kappa students at Cambridge, "Fear always springs from ignorance."[61] The story of Slammer's infection of a nuclear power plant loses much of its punch when the full picture is revealed: the plant was offline, and had been for nearly a year, when the worm struck;[62] the failed monitoring system had an analog backup system that was not compromised;[63] no disruptions in service or power outages were traced to Slammer;[64] and the vulnerability that Slammer

[53] Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Net*, REGISTER (Aug. 20, 2003), http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/.

[54] *Id.*

[55] *Id.*

[56] RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 99 (2010).

[57] Poulsen, *supra* note 53.

[58] CLARKE & KNAKE, *supra* note 56, at 99.

[59] *Id.*

[60] Marcelo Soares, *Brazilian Blackout Traced to Sooty Insulators, Not Hackers*, WIRED (Nov. 9, 2009), http://www.wired.com/threatlevel/2009/11/brazil_blackout/.

[61] Ralph Waldo Emerson, The American Scholar, Address Before the Phi Beta Kappa Society at Cambridge (Aug. 1837), *in* THE AMERICAN SCHOLAR 40 (1901).

[62] Poulsen, *supra* note 53.

[63] *Id.*

[64] N. AM. ELEC. RELIABILITY COUNCIL, SQL SLAMMER WORM LESSONS LEARNED FOR CONSIDERATION BY THE ELECTRICITY SECTOR (2003).

exploited was so well-known that Microsoft had deployed a patch fixing the problem six months before Slammer was released.[65]

B. SCADA Security and Stuxnet

Even the true version of the Slammer tale highlights a larger, and more realistic, problem: the computer systems that run much of America's industrial processes are truly archaic. Supervisory control and data acquisition (SCADA) systems are used to monitor and control critical industrial processes like power generation.[66] A variety of industries across the United States employ some form of SCADA system.[67] SCADA systems were developed in the 1960s, and many systems based in whole or in part on that initial design remain in use today.[68] These technological dinosaurs were never designed to interface with massive corporate intranets that put SCADA systems within reach of the Internet and all its cyber pathogens.[69] Stuxnet was such a pathogen, and its saga has helped propel SCADA security issues to the forefront of the cybersecurity debate.

Stuxnet, discovered on July 14, 2010,[70] was "one of the most sophisticated and unusual pieces of malicious software ever created" and was "the first worm built not only to spy on industrial systems, but also to

[65] Poulsen, *supra* note 53. The existence of the patch was undoubtedly interesting news to FirstEnergy's network administrators, who had failed to apply the update in the six months after its release. *Id.*

[66] WILLIAM T. SHAW, CYBERSECURITY FOR SCADA SYSTEMS 3 (2006).

[67] *See* JACK WILES ET AL., TECHNO SECURITY'S GUIDE TO SECURING SCADA 62–64 tbls.2.1 & 2.2 (2007) (listing SCADA-reliant industries and the various functions SCADA systems perform within them). Electric companies were early adopters of SCADA systems and continue to be major users today. SHAW, *supra* note 66, at 335. There is even a boutique industry dedicated to supplying these companies with legacy hardware, software, and support because the original manufacturers either no longer exist or have moved on to more advanced models. *Id.* at 336. Many of these legacy SCADA systems employ analog telephone lines for data distribution and transmit at speeds far slower than modern network technologies. *Id.*

[68] SHAW, *supra* note 66, at 4–5.

[69] *See* WILES ET AL., *supra* note 67, at 74 ("Basically, SCADA systems have no inherent ability to cope with the issues commonly found plaguing today's enterprise networks. Connecting the SCADA system to a corporate network dramatically increases risks poised [sic] by traditional malware. . . . [M]ost of the current installed base of SCADA systems in use today utilize protocols that are either inherently insecure by design or that by-and-of themselves are not necessarily insecure but are poorly implemented by the SCADA product vendor, which results in SCADA insecurities."). The limitations built into SCADA systems are so significant that manuals for diagnosing and addressing their weaknesses actually recommend *against* virus scanning systems more than five years old in order to avoid crashing the system outright. *Id.* at 76. Despite these concerns, SCADA systems often have life spans in excess of twenty years. Garett Montgomery, *SCADA: Threat Landscape* 4 (May 18, 2010), http://cio.energy.gov/documents/Cracking_Down_SCADA_Security_-_Garret_Montgomery.pdf.

[70] Robert McMillan, *New Spy Rootkit Targets Industrial Secrets*, TECHWORLD (July 19, 2010), http://news.techworld.com/security/3232365/new-spy-rootkit-targets-industrial-secrets/.

reprogram them."[71] The worm spread like a traditional Windows-based rootkit but was uniquely targeted at specific SCADA subsystems.[72] Though tens of thousands of computers were ultimately infected with Stuxnet,[73] the "epicenter" of the infection was Iran,[74] where it targeted five Iranian "industrial processing organisations."[75] Some security experts speculate that the final target was Iran's Bushehr nuclear power plant,[76] a fear confirmed at least in part by the Iranian government.[77]

Though Stuxnet's sophistication and specificity are indeed a cause for concern, once again, the risks were blown out of proportion by the media and their cybersecurity sources. "[W]e can expect that something will blow up soon . . . . Something big," quipped one analyst.[78] Rumors of nation-state involvement quickly circulated,[79] with accusations leveled at Israel.[80] Yet Siemens, the manufacturer of the targeted machines, reported that no plant operations had been disrupted as a result of Stuxnet.[81] Further, the Siemens systems used in Iran were modified and illegally acquired,[82] meaning they lack even the imperfect security measures typical of SCADA systems. Put

[71] Robert McMillan, *Siemens: Stuxnet Worm Hit Industrial Systems*, COMPUTERWORLD (Sept. 14, 2010), http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems.

[72] Nicolas Falliere, *Stuxnet Introduces the First Known Rootkit for Industrial Control Systems*, SYMANTEC OFFICIAL BLOG (Aug. 19, 2010), http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

[73] *See* Mark Clayton, *Stuxnet Malware is "Weapon" out to Destroy . . . Iran's Bushehr Nuclear Plant?*, CHRISTIAN SCI. MONITOR (Sept. 21, 2010), http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant (referencing a Microsoft report that at least 45,000 computers had been infected worldwide as of August 2010).

[74] *Id.*

[75] Jonathan Fildes, *Stuxnet Virus Targets and Spread Revealed*, BBC NEWS (Feb. 15, 2011), http://www.bbc.co.uk/news/technology-12465688 (internal quotation marks omitted).

[76] *E.g.*, John Markoff, *Iran Worm Can Deal Double Blow to Nuclear Program*, N.Y. TIMES, Nov. 20, 2010, *available at* http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html; Clayton, *supra* note 73.

[77] *Iran Confirms Stuxnet Worm Halted Centrifuges*, CBS NEWS (Nov. 29, 2010), http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml.

[78] Clayton, *supra* note 73.

[79] Jonathan Fildes, *Stuxnet Worm "Targeted High-Value Iranian Assets,"* BBC NEWS (Sept. 23, 2010), http://www.bbc.co.uk/news/technology-11388018; McMillan, *supra* note 71.

[80] William J. Broad et al., *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[81] McMillan, *supra* note 71. Circumstantial evidence may support the claim that Stuxnet led to the destruction of roughly one thousand Iranian centrifuges at the Natanz uranium-enrichment facility, but Iran's actual output of enriched uranium was ultimately unaffected. DAVID ALBRIGHT ET AL., STUXNET MALWARE AND NATANZ: UPDATE OF ISIS DECEMBER 22, 2010 REPORT 1–5 (2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/02/stuxnet-update-feb-15-2011-final.pdf.

[82] *Cf.* Kim Zetter, *Surveillance Footage and Code Clues Indicate Stuxnet Hit Iran*, WIRED (Feb. 16, 2011), http://www.wired.com/threatlevel/2011/02/isis-report-stuxnet (concluding that a number of companies are involved in illegally acquiring parts for Iran's nuclear program in violation of nonproliferation agreements).

bluntly, hacking into the Iranian nuclear infrastructure is likely considerably easier than infiltrating similar American systems.

C. Information Thieves

Internet-based threats are not only about crippling infrastructure and disabling important systems. Information security is a prime consideration for many web-connected entities, and for good reason. In December 2010, Google was on the receiving end of a cyber attack intended to give the perpetrators access to the Gmail accounts of various Chinese human rights activists.[83] Analysts believe the attackers sent e-mails to Google employees, attaching PDF files containing hidden software that automatically (but discreetly) installed itself when the documents were opened.[84] Once installed, the software gave the attackers the ability to explore some of Google's internal systems.[85] Google responded by announcing that it was reconsidering its entire operation in China.[86] The search giant's exit from the country is "now 99.9 per cent certain."[87]

Google is not the only company with security troubles. In March 2011, RSA, the computer-security division of EMC Corporation, was also attacked.[88] The RSA hack took advantage of unwary employees, enticing them to open spreadsheets laced with malicious code.[89] Once inside, the hackers extracted information related to the company's SecurID authentication products,[90] which some forty million businesses use to add

[83] David Drummond, *A New Approach to China*, OFFICIAL GOOGLE BLOG (Jan. 12, 2010, 3:00 PM), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html. Google was one of "at least twenty other large companies" targeted. *Id.* Software purveyor Adobe was also among the victims. Pooja Prasad, *Adobe Investigates Corporate Network Security Issue*, ADOBE FEATURED BLOGS (Jan. 12, 2010, 3:16 PM), http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html.

[84] John Leyden, *Security Experts Dissect Google China Attack*, REGISTER (Jan. 14, 2010), http://www.theregister.co.uk/2010/01/14/google_china_attack_analysis/.

[85] *Id.*

[86] Drummond, *supra* note 83.

[87] Kathrin Hille & Richard Waters, *Google "99% Certain" to Shut China Search Engine*, FIN. TIMES, Mar. 13, 2010 (internal quotation marks omitted), *available at* http://www.ft.com/cms/s/2/dd69e680-2e06-11df-b85c-00144feabdc0.html; *see also* Michael B. Farrell, *What a Google China Exit Would Mean*, CHRISTIAN SCI. MONITOR (Mar. 16, 2010), http://www.csmonitor.com/USA/2010/0316/What-a-Google-China-exit-would-mean (positing that Google appears to be shutting down its China operations).

[88] Tim Stevens, *RSA Hacked, Data Exposed that Could "Reduce the Effectiveness" of SecurID Tokens*, ENGADGET (Mar. 18, 2011, 8:49 AM), http://www.engadget.com/2011/03/18/rsa-hacked-data-exposed-that-could-reduce-the-effectiveness-o/.

[89] Riva Richmond, *The RSA Hack: How They Did It*, BITS (Apr. 2, 2011, 3:17 PM), http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/. The security flaw in Adobe's Flash software that enabled the attack has since been fixed. *Id.*

[90] Arthur W. Coviello, Jr., *Open Letter to RSA Customers*, RSA, http://www.rsa.com/node.aspx?id=3872.

another layer of protection to their networks.[91] Though RSA insists the stolen information "does not enable a successful direct attack on any of [their] RSA SecurID customers,"[92] the incident does illustrate that no one—not even a security expert—is invincible.

D. Hacktivism

Though the idea of "hacktivism"—"[c]ommonly defined as the marriage of political activism and computer hacking"[93]—is at least twenty years old,[94] it may become the new vogue going forward.[95] In 2010, WikiLeaks[96] gained notoriety for distributing hundreds of thousands of "confidential American diplomatic cables" via its website.[97] The controversial leaks made the organization both famous and infamous, subjecting founder Julian Assange to criticism[98] and criminal investigation.[99]

Meanwhile the WikiLeaks website was struggling to stay connected in the face of multiple distribute denial-of-service (DDoS) attacks.[100] Fighting

[91] Richmond, *supra* note 89. SecurID products often take the form of a palm-sized "token," which provides a constantly changing numeric code that users must append to their passwords in order to access protected systems. John Markoff, *SecurID Company Suffers a Breach of Data Security*, N.Y. TIMES, Mar. 18, 2011, *available at* http://www.nytimes.com/2011/03/18/technology/18secure.html.

[92] Coviello, *supra* note 90.

[93] Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation (Sept. 2004) (unpublished Ph.D. thesis, Harvard University), *available at* http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.

[94] Julian Assange, *The Curious Origins of Political Hacktivism*, COUNTERPUNCH, Nov. 26–27, 2006, *available at* http://www.counterpunch.org/2006/11/25/the-curious-origins-of-political-hacktivism/.

[95] MCAFEE LABS, *supra* note 24, at 6 ("Hacktivism will become the new way to demonstrate your political position in 2011 and beyond."). The governments of Tunisia and Zimbabwe were recently attacked—digitally—in protest of government censorship. *Anonymous Activists Target Tunisian Government Sites*, BBC NEWS, http://www.bbc.co.uk/news/technology-12110892 (last updated Jan. 4, 2011).

[96] WikiLeaks describes itself as "a not-for-profit media organisation." *About*, WIKILEAKS, http://wikileaks.ch/About.html.

[97] Much of the leaked material is now available on the *New York Times*' website. *State's Secrets*, N.Y. TIMES, http://www.nytimes.com/interactive/world/statessecrets.html (last updated Nov. 29, 2010). Other leaked documents included "protocols from Guantánamo Bay" and "9/11 pager messages." *WikiLeaks*, N.Y. TIMES, http://topics.nytimes.com/top/reference/timestopics/organizations/w/wikileaks/index.html (last updated Aug. 30, 2011).

[98] *See, e.g.*, Alexandra Topping & Jo Adetunji, *Afghanistan War Logs: WikiLeaks Founder Rebuts White House Criticism*, GUARDIAN (July 26, 2010), http://www.guardian.co.uk/world/2010/jul/26/war-logs-wikileaks-rebuts-criticism (recounting the White House's criticism of Assange for leaking documents that "could put the lives of Americans and our partners at risk, and threaten our national security").

[99] Kim Zetter, *Report: Federal Grand Jury Considering Charges Against WikiLeaks' Assange*, WIRED (Dec. 13, 2010), http://www.wired.com/threatlevel/2010/12/assange-grand-jury/ (detailing a number of potential charges Assange could face).

[100] M. Alex Johnson, *DDoS Attack on WikiLeaks Gathers Strength*, TECHNOLOG (Dec. 1, 2010, 2:43 PM), http://technolog.msnbc.msn.com/_news/2010/12/01/5561895-ddos-attack-on-wikileaks-gathers-strength; *see also @wikileaks*, TWITTER (Nov. 30, 2010), http://twitter.com/

fire with fire, WikiLeaks supporters in the online group "Anonymous" launched "Operation Payback," orchestrating DDoS attacks of their own against MasterCard,[101] Visa,[102] and PayPal[103] (for suspending donations to WikiLeaks) and flirted with attacking Amazon (for taking down the WikiLeaks site hosted on its servers).[104]

As interesting as the political dimensions of the WikiLeaks saga are,[105] the most intriguing aspect of the DDoS wave was its *voluntary* nature. Traditional DDoS attacks remotely activate armies of infected computers, known as "zombies," to create digital traffic jams in an instant.[106] What makes Anonymous's attacks unique is that individuals "infected" themselves by voluntarily downloading the botnet software.[107] If voluntary DDoS attacks become a new trend,[108] preparations to deal with them become all the more important.

* * *

The preceding examples are but a few chosen from many,[109] yet they serve to illustrate the varied and ever-changing threats facing America's networks. Alarmist rhetoric, perhaps intended to spur lawmakers to action, often has the opposite effect because the proposals attempt to match the

wikileaks/statuses/9578593516523520 ("We are currently under another DDOS attack."). DDoS attacks vary significantly in character, but the traditional form involves flooding web servers with requests for information in order to overload the system and cut off access to the site. *See infra* note 106 and accompanying text. Some have theorized that the DDoS attacks against WikiLeaks were more sophisticated, exploiting weaknesses in server technology rather than relying on brute force. *E.g.*, John Leyden, *WikiLeaks Hit by Second DDoS*, REGISTER (Nov. 30, 2010), http://www.theregister.co.uk/2010/11/30/wikileaks_ddos_again/.

[101] Esther Addley & Josh Halliday, *Operation Payback Cripples MasterCard Site in Revenge for WikiLeaks Ban*, GUARDIAN (Dec. 8, 2010), http://www.guardian.co.uk/media/2010/dec/08/operation-payback-mastercard-website-wikileaks; Keith Weir, *WikiLeaks Backers Hit MasterCard and Visa in Cyberstrike*, REUTERS (Dec. 8, 2010), http://www.reuters.com/article/2010/12/08/us-wikileaks-idUSL3E6N80HH20101208.

[102] *Anonymous Hacktivists Say WikiLeaks War to Continue*, BBC NEWS, http://www.bbc.co.uk/news/technology-11935539 (last updated Dec. 9, 2010) [hereinafter *Anonymous Hacktivists*]; Weir, *supra* note 101.

[103] *Pro-WikiLeaks Activists Abandon Amazon Cyber Attack*, BBC NEWS, http://www.bbc.co.uk/news/technology-11957367 (last updated Dec. 9, 2010) [hereinafter *Amazon Cyber Attacks*].

[104] *Id.*

[105] *See generally* Samuel, *supra* note 93 (exploring the role of hacktivism in political participation).

[106] Mary Landesman, *What Is a DDoS Attack?*, ABOUT.COM, http://antivirus.about.com/od/whatisavirus/a/ddosattacks.htm.

[107] *Anonymous Hacktivists*, *supra* note 102; *Amazon Cyber Attacks*, *supra* note 103.

[108] Hacktivists have rarely used DDoS attacks in the past. Samuel, *supra* note 93, at 10. However, the WikiLeaks saga may signal a paradigm shift.

[109] *See Significant Cyber Incidents Since 2006*, CTR. FOR STRATEGIC & INT'L STUDIES, http://csis.org/files/publication/110906_Significant_Cyber_Incidents_Since_2006.pdf (last modified Sept. 6, 2011) (listing over eighty cyber incidents since 2006).

severity of the alleged threat.[110] Wildly speculating about terrorist plots[111] and a "cyber 9/11"[112] frames the debate too dramatically. Politicians who do not understand the underlying technologies that they want to regulate also exacerbate the problem.[113] Though the reality of the danger is undeniable, Americans need not abandon their favorite technologies, nor companies hand the keys to their server rooms over to the government for massive regulation. Yet a review of the current legal and regulatory landscape reveals that these modern technological threats are being crudely addressed with old-world tools that are incapable of producing the desired results.

[110] *See, e.g.*, Brendan Koerner, *Bush's Cyberstrategery*, SLATE (Mar. 3, 2003), http://www.slate.com/id/2079549/ (noting that President George W. Bush's 2003 National Strategy to Secure Cyberspace is "chock full of what computer-security experts term 'FUD'—geek shorthand for spreading bogus 'fear, uncertainty, and doubt'").

[111] *See* SENATE COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010, S. REP. NO. 111-368, at 3, 5, 10 (2010) (alleging that companies have been victims of terrorist infiltrations and warning of "cyber-terrorism"); *Cyber Security: Developing a National Strategy: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. 93 (2009) (statement of Alan Paller, Director of Research, SANS Institute) [hereinafter Paller Testimony] ("Terrorist organizations also have run hacking schools in Afghanistan and in other countries and use other methods to teach their recruits to hack into computers."). Yet even the hawkish Richard Clarke admits that "[c]yber terrorism is largely a red herring." CLARKE & KNAKE, *supra* note 56, at 135–36 ("Indeed, we do not have any good evidence that terrorists have ever staged cyber war attacks on infrastructure.").

[112] *See supra* note 46 and accompanying text.

[113] Perhaps the best-known example of congressional technological ignorance is a gaffe by the late Senator Ted Stevens. At 83 years of age, Stevens served as Chair of the Senate Committee on Commerce, Science, and Transportation—the committee with jurisdiction over communications issues. *Stevens, Theodore Fulton (Ted)*, BIOGRAPHICAL DIRECTORY OF THE U.S. CONGRESS, http://bioguide.congress.gov/scripts/biodisplay.pl?index=s000888; *Jurisdiction*, U.S. SENATE COMMITTEE ON COM., SCI., & TRANSP., http://commerce.senate.gov/public/index.cfm?p=Jurisdiction. During a debate over a net neutrality amendment to a telecommunications bill, Stevens let his (mis)understanding of the Internet slip:

> I just the other day got, an internet was sent by my staff at 10 o'clock in the morning on Friday and I just got it yesterday.
>
> Why?
>
> Because it got tangled up with all these things going on the internet commercially.
>
> . . .
>
> And again, the internet is not something you just dump something on. It's not a truck.
>
> It's a series of tubes.

Your Own Personal Internet, WIRED (June 30, 2006), http://www.wired.com/threatlevel/2006/06/your_own_person/. The "series of tubes" line was widely lampooned and used to illustrate how out of touch Congress was with technology. *See, e.g.*, Alexandra Petri, *Sen. Stevens, the Tubes Salute You*, POSTPARTISAN (Aug. 10, 2010, 3:06 PM), http://voices.washingtonpost.com/postpartisan/2010/08/senator_stevens_the_tubes_salu.html ("This was the gaffe heard round the 'net, igniting a response that spanned every news outlet from Fark to the New York Times."); *Series of Tubes: Pop Culture References*, WIKIPEDIA, http://en.wikipedia.org/wiki/Series_of_tubes#Pop_culture_references (last modified Oct. 11, 2011) (describing various pop-culture references to the "series of tubes" phrase). Similar criticism has been leveled at Congress broadly. *See* Declan McCullagh, *Cybersecurity Bill Gives DHS Power to Punish Tech Firms*, CNET NEWS (Nov. 19, 2010), http://news.cnet.com/8301-13578_3-20023464-38.html ("Congress is stepping forward to regulate something it has no idea how to regulate." (quoting Jim Harper, policy analyst at the Cato Institute)).

IV. Current Approaches to Cybersecurity

A. Executive Emergency Powers: The Communications Act of 1934

Long before ARPA and the creation of the Internet,[114] the Federal Communications Commission (FCC) was created "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available . . . to all the people of the United States . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service."[115] As communications technologies developed and expanded, so too did the FCC's regulatory reach.[116] Because the language of the Communications Act of 1934 is so broad,[117] courts have allowed the FCC similarly broad (though not unlimited) authority to regulate, for example, cable television.[118] The scope of the FCC's authority to regulate the Internet remains an open question.[119]

But direct regulation of the Internet by the FCC is not inherently troubling. What is troubling is § 706 of the Communications Act,[120] which

[114] *See supra* subpart II(A).

[115] Communications Act of 1934 § 1, 47 U.S.C. § 151 (2006).

[116] *See History of Communications*, FCC, http://www.fcc.gov/omd/history (last updated Nov. 21, 2005) ("[W]hile the formal charge of Congress to the FCC can be summed up in less than 30 words—ensure that the American people have available, at reasonable costs and without discrimination, rapid, efficient, Nation- and world-wide communication services; whether by radio, television, wire, satellite, or cable—the day-to-day reality may be that there is no more ubiquitous presence in the lives of most Americans than the FCC-regulated communications industries.").

[117] *See* Communications Act of 1934 § 2(a), 47 U.S.C. § 152(a) (2006) ("The provisions of this chapter shall apply to all interstate and foreign communication by wire or radio . . . .").

[118] *See, e.g.*, United States v. Midwest Video Corp. (*Midwest Video I*), 406 U.S. 649, 670 (1972) (upholding an FCC regulation requiring cable providers to provide local origination facilities); United States v. Sw. Cable Co., 392 U.S. 157, 172–73 (1968) ("Nothing in the language of § 152 (a), in the surrounding language, or in the Act's history or purposes limits the Commission's authority to those activities and forms of communication that are specifically described by the Act's other provisions. . . . [T]he legislative history indicates that . . . Congress . . . conferred upon the Commission a 'unified jurisdiction' and 'broad authority.' . . . Congress in 1934 acted in a field that was demonstrably 'both new and dynamic,' and it therefore gave the Commission 'a comprehensive mandate,' with 'not niggardly but expansive powers.' We have found no reason to believe that § 152 does not, as its terms suggest, confer regulatory authority over 'all interstate . . . communication by wire or radio.'" (footnotes omitted) (citations omitted)). *But see* FCC v. Midwest Video Corp. (*Midwest Video II*), 440 U.S. 689, 708 (1979) (striking down FCC regulations mandating public access to broadcast facilities). After *Midwest Video II*, Congress modified the Communications Act to explicitly provide for regulation of cable television. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified as amended at 47 U.S.C. §§ 521–573 (2006)).

[119] *See, e.g.*, Comcast Corp. v. FCC, 600 F.3d 642, 661 (D.C. Cir. 2010) (vacating an FCC order attempting to regulate Comcast's Internet services). *See generally* James B. Speta, *FCC Authority to Regulate the Internet: Creating It and Limiting It*, 35 LOY. U. CHI. L.J. 15 (2003) (discussing differing approaches to FCC regulation of the Internet).

[120] Communications Act of 1934 § 706, 47 U.S.C. § 606 (2006). The FCC has acknowledged that its "interest in cybersecurity is rooted in the Communications Act of 1934." Bill Lane, *Tech Topic 20: Cyber Security and Communications*, FCC, http://www.fcc.gov/pshs/techtopics/techtopics20.html.

provides the President with broad emergency powers during times of war or "national emergency."[121] In such a scenario, the President has free rein to ignore the regulations affecting communications systems, close facilities, remove equipment, and authorize government control of the systems.[122] Section 706 is open to interpretation as an outright Internet kill switch.[123] Indeed, officials within the Department of Homeland Security have already acknowledged that § 706 allows for the President to take "extraordinary measures" to respond to "cyber threats."[124] Others have recognized that "in the event of a cyber attack, the President's authorities are broad and ambiguous—a recipe for encroachments on privacy and civil liberties."[125]

Using § 706 to (temporarily) nationalize America's Internet infrastructure appears to be consistent with longstanding theories of executive power. In what has been called "the most truly intellectually satisfying" judicial opinion in American history, *Youngstown Sheet & Tube Co. v. Sawyer*,[126] Justice Jackson established his "famous tripartite analysis" for questions of executive power.[127] According to Jackson, executive power reaches its apex when the President acts "pursuant to an express or implied authorization of Congress."[128] Since § 706 expressly provides the President with the authority to commandeer wire-communication facilities during a "state or threat of war,"[129] the only impediment to a government takeover is a declaration by the President that such a state or threat exists. Given the frequent retreat by government officials to claims of terrorism or state-sponsored cyber warfare,[130] it is foreseeable that a President could make such a declaration given the right political climate. Lending credence to these

[121] 47 U.S.C. § 606(c).

[122] *Id.*

[123] Alan Paller, *President Has Had 'Kill Switch' for Communications Since 1934*, GOV'T COMPUTER NEWS (June 28, 2010), http://gcn.com/articles/2010/06/28/no--kill-switch-in-lieberman-collins-bill.aspx.

[124] *Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. (2010) (statement of Philip Reitinger, Deputy Under Secretary, National Protection & Programs Directorate, Department of Homeland Security) [hereinafter Reitinger Testimony].

[125] 157 CONG. REC. S910 (daily ed. Feb. 17, 2011) (statement of Sen. Collins).

[126] 343 U.S. 579 (1952).

[127] Sanford Levinson, *The Rhetoric of the Judicial Opinion*, *in* LAW'S STORIES: NARRATIVE AND RHETORIC IN THE LAW 187, 202–03 (Peter Brooks & Paul Gewirtz eds., 1996).

[128] *Youngstown*, 343 U.S. at 635. "A seizure executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it." *Id.* at 637.

[129] Communications Act of 1934 § 706(c), 47 U.S.C. § 606(c) (2006).

[130] *See supra* notes 109–11 and accompanying text.

suspicions, the Pentagon recently declared that a cyber attack can constitute an "act of war."[131]

B. Presidential Cybersecurity Policies

Though not a lawmaking body, the Executive Branch does play an active role in shaping national policy on any number of issues. Throughout the years, presidents have used Presidential Directives to communicate executive policy preferences.[132] Whatever the name,[133] Presidential Directives have the same substantive legal effect as executive orders.[134]

In 1998, President Clinton issued Presidential Decision Directive (PDD) 63, which created the National Infrastructure Protection Center (NIPC) within the Federal Bureau of Investigation (FBI).[135] NIPC was to focus on protecting the nation's "critical infrastructure" from computer-based attacks, "facilitating and coordinating" the government's infrastructure-protection policies, monitoring threats, and overseeing recovery efforts in the event of an attack.[136] Notwithstanding the coordinating role of NIPC, PDD-63 made clear that individual federal agencies were responsible for securing their own critical systems.[137] PDD-63 also placed importance on a public–private partnership through which the government and private companies would work together to prevent cyber attacks.[138]

[131] Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, *available at* http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

[132] HAROLD C. RELYEA, PRESIDENTIAL DIRECTIVES: BACKGROUND AND OVERVIEW 3 (2008); George Caldwell, *Presidential Directives and Where to Find Them*, LIBRARY OF CONGRESS, http://www.loc.gov/rr/news/directives.html (last updated Mar. 13, 1998).

[133] Presidential Directives have been known as National Security Action Memoranda (Kennedy & Johnson), National Security Decision Memoranda (Nixon & Ford), Presidential Directives (Carter), National Security Decision Directives (Reagan), National Security Directives (G.H.W. Bush), Presidential Decision Directives (Clinton) and National Security Presidential Directives (G.W. Bush). Caldwell, *supra* note 132. The practice, under any name, dates back to George Washington. RELYEA, *supra* note 132, at 1.

[134] Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order, 24 Op. O.L.C. 29, 29 (2000). Undefined by the Constitution or by statute, executive orders operate as a type of "Presidential legislation." John E. Noyes, *Executive Orders, Presidential Intent, and Private Rights of Action*, 59 TEXAS L. REV. 837, 839 (1981) (internal quotation marks omitted).

[135] U.S. DEP'T OF JUSTICE, THE CLINTON ADMINISTRATION'S POLICY ON CRITICAL INFRASTRUCTURE PROTECTION: PRESIDENTIAL DECISION DIRECTIVE 63, at 9–10 (1998) [hereinafter PDD WHITE PAPER], *available at* http://www.justice.gov/criminal/cybercrime/white_pr.htm.

[136] *Id.*

[137] *Id.* at 5 ("Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems.").

[138] *Id.* at 10.

President George W. Bush continued the legacy of PDD-63 with National Security Presidential Directive (NSPD) 38,[139] which implemented 2003's "National Strategy to Secure Cyberspace."[140] That national strategy spanned seventy-six pages and set five major priorities: (1) charging the recently created Department of Homeland Security with responding to attacks and providing guidance on cybersecurity strategies;[141] (2) improving cybercrime enforcement and strengthening systems against potential threats;[142] (3) improving nationwide knowledge regarding cybersecurity issues through educational and training programs;[143] (4) securing government systems;[144] and (5) incorporating cybersecurity into the country's national security policy at home and abroad.[145] The common themes of coordination and public–private partnerships appeared throughout.[146]

The year 2008 brought with it President Bush's NSPD-54, establishing the Comprehensive National Cybersecurity Initiative (CNCI) (though NSPD-54 remained classified until March 2010).[147] The Obama Administration has embraced and expanded the CNCI; its twelve active "initiatives" focus on developing hardware- and software-based security upgrades for federal systems,[148] improving communication and education,[149] and partnering with the private sector to protect critical infrastructure.[150] President Obama also ordered a sixty-day "comprehensive, 'clean-slate' review" of national

[139] Steven Aftergood, *National Security Presidential Directives, George W. Bush Administration*, FEDERATION OF AMERICAN SCIENTISTS (Mar. 2, 2010), http://www.fas.org/irp/offdocs/nspd/index.html.

[140] *See generally* U.S. COMPUTER EMERGENCY READINESS TEAM, U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003) [hereinafter 2003 NATIONAL STRATEGY], *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

[141] *Id.* at 19–25.

[142] *Id.* at 27–35.

[143] *Id.* at 37–42.

[144] *Id.* at 43–48.

[145] *Id.* at 49–52.

[146] *See, e.g.*, *id.* at 32 (calling on DHS and the Department of Energy to work with the private sector to promote SCADA-security improvements).

[147] Adam R. Pearlman, Federal Cybersecurity Programs 2 (Aug. 12, 2010) (unpublished manuscript), *available at* http://ssrn.com/abstract_id=1655105. Such secrecy was not uncommon.

> Of the 54 National Security Presidential Directives issued by the Bush Administration to date, the titles of only about half have been publicly identified. There is descriptive material or actual text in the public domain for only about a third. In other words, there are dozens of undisclosed Presidential directives that define U.S. national security policy and task government agencies, but whose substance is unknown either to the public or, as a rule, to Congress.

Steven Aftergood, *The Next President Should Open Up the Bush Administration's Record*, NIEMAN WATCHDOG (Feb. 7, 2008), http://niemanwatchdog.org/index.cfm?fuseaction=ask_this.view&askthisid=00321.

[148] EXEC. OFFICE OF THE PRESIDENT OF THE U.S., THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE 2–3 [hereinafter CNCI], *available at* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[149] *Id.* at 3–4.

[150] *Id.* at 4–5.

cybersecurity policy,[151] which yielded a seventy-six-page cybersecurity approach largely indistinguishable from President Bush's 2003 plan.[152]

Several trends can be distilled from the last decade of presidential cybersecurity policy. Naturally, the Executive Branch prefers to retain control over the direction of cybersecurity policy by locating leadership within the White House.[153] Public–private partnerships are a recurring theme, focusing on persuading private entities to help the government protect critical infrastructure, most of which is privately owned.[154] Executive Branch policy also emphasizes communication and coordination, perhaps because the White House continues to bring more and more of the government bureaucracy into the cybersecurity fold.

C. Congressional Cybersecurity Policies

Not content to let the Executive Branch dominate the future of Internet regulation, the 112th Congress has at least seven different cybersecurity bills pending before it.

1. Cyber Security and American Cyber Competitiveness Act of 2011.— Perhaps the least ambitious proposal on the table is S. 21, the Cyber Security and American Cyber Competitiveness Act of 2011 (CSACCA).[155] The bill spans just five pages, two of which are dedicated to describing the cybersecurity problem in broad, unsubstantiated terms.[156] The thrust of the legislation is merely a call to action: "Congress should enact . . . bipartisan legislation to secure the United States against cyber attack" by improving security, incentivizing private companies to defend themselves, investing in tech-sector jobs, and defending critical infrastructure, all while protecting the civil liberties of American citizens.[157] Those are noble goals, but not ones that CSACCA itself appears to be capable of achieving.

2. Cybersecurity and Internet Safety Standards Act.—Similarly uninspiring is the Cybersecurity and Internet Safety Standards Act

[151] CYBERSPACE POLICY REVIEW, *supra* note 47, at iii.

[152] Declan McCullagh, *A Cybersecurity Quiz: Can You Tell Obama From Bush?*, CNET NEWS (May 29, 2009), http://news.cnet.com/8301-13578_3-10252263-38.html ("[T]he two reports are remarkably similar. Perhaps this should be no surprise: Obama selected Melissa Hathaway, who worked for the director of national intelligence in the Bush administration and was director of a[] Bush-era 'Cyber Task Force,' to conduct the review.").

[153] Pearlman, *supra* note 147, at 4.

[154] Alexandra Marks, *How Should US Protect Privately Owned Facilities?*, CHRISTIAN SCI. MONITOR (June 5, 2007), http://www.csmonitor.com/2007/0605/p01s03-usgn.html.

[155] Cyber Security and American Cyber Competitiveness Act of 2011, S. 21, 112th Cong. (2011).

[156] *See id.* § 2(3) (claiming that American companies have already lost over one trillion dollars of intellectual property to malicious attackers).

[157] *Id.* § 3.

(CISSA).[158] The bill stresses the creation of "minimum voluntary or mandatory cybersecurity and Internet safety standards."[159] Unfortunately, rather than proposing concrete solutions, CISSA proposes that the Secretary of the Department of Homeland Security conduct a massive "cost-benefit analysis" considering "all relevant factors" and "legal impediments" to the development and implementation of security standards by Internet service providers (ISPs).[160] As this Note partially demonstrates, the debate is already framed, the problem well-known, the stage set. A year-long study serves only to delay imminently necessary regulation.

3. *Cybersecurity Education Enhancement Act of 2011*.—The first of the material solutions before Congress is the Cybersecurity Education Enhancement Act of 2011 (CEEA).[161] CEEA proposes a long-term, partial solution to the cybersecurity dilemma by establishing a $3.7 million grant program to encourage universities to create and expand advanced programs in cybersecurity.[162] The bill would also create an "E-Security Fellows Program," through which public- and private-sector employees in relevant fields could work directly with the Department of Homeland Security on cybersecurity matters.[163]

4. *Chief Technology Officer Act*.—Taking a page from President Obama's cybersecurity review,[164] the Chief Technology Officer Act (CTOA) would establish the Office of the Federal Chief Technology Officer within the Executive Office of the President.[165] Headed by a presidential appointee, the Chief would become the cybersecurity go-to person for both the President and the government at large.[166] The Office of the Federal Chief Technology Officer would largely design and coordinate policy for federal agencies; even the "public-private sector partnership initiatives" the Office would be charged with forging are intended to expose the government to private-sector innovations.[167] While this solution would provide the centralization of authority and oversight that is needed, relying upon existing market-power

[158] Cybersecurity and Internet Safety Standards Act, S. 372, 112th Cong. (2011).

[159] *Id.* § 3(3).

[160] *Id.* § 4.

[161] Cybersecurity Education Enhancement Act of 2011, H.R. 76, 112th Cong. (2011).

[162] *Id.* § 2(a), (e).

[163] *Id.* § 3.

[164] *See supra* notes 148–52 and accompanying text.

[165] Chief Technology Officer Act, H.R. 1261, 112th Cong. § 2(a)(1)(A) (2011).

[166] *See id.* § 2(b) (listing the duties of the Chief Technology Officer).

[167] *See id.* § 2(b)(9)–(10) (stating that the Federal Chief Technology Officer would have a duty to establish public–private partnerships for the purposes of improving government knowledge of current and developing technologies).

incentives and failing to directly address private-sector vulnerabilities is not likely to achieve the nation's cybersecurity goals.[168]

5. Cyber Security Public Awareness Act of 2011.—Though the short title suggests an emphasis on informing the public, the Cyber Security Public Awareness Act (CSPAA) is really concerned with providing Congress with access to data on cyber attacks across the nation. The first of several reports required by the bill is a Department of Homeland Security report summarizing "major cyber incidents involving networks of executive agencies,"[169] and a Department of Defense report covering the same topics with regards to defense and military networks.[170] DHS would also be required to provide reports assessing the security risks facing the nation's electric grid[171] and those posed by technologies acquired from foreign countries.[172] Major industries would be called upon to provide their own cyber incident reports via their "primary regulators," such as the Federal Energy Regulatory Commission and the Federal Communications Commission.[173] The FBI and the Attorney General would provide Congress with information on cybercrime-related prosecutions,[174] while the Securities and Exchange Commission would weigh in on the impact of cyber attacks on the financial sector.[175] CSPAA would task the Secretary of Homeland Security with publishing a number of additional reports, detailing (1) ways in which federal agencies could assist the private sector in defending "information networks,"[176] (2) methods for protecting "critical infrastructure,"[177] and (3) plans to promote and improve public awareness of cybersecurity issues generally.[178]

6. Homeland Security Cyber and Physical Infrastructure Protection Act of 2011.—One of the more comprehensive proposals on the table, the Homeland Security Cyber and Physical Protection Act of 2011 (HSCPIPA), would refocus the Office of Cybersecurity and Communications (OCC) within the Department of Homeland Security.[179] OCC would "establish and enforce cybersecurity requirements for civilian nonmilitary and nonintelli-

[168] *See infra* section V(C)(2) (arguing that private-sector systems are vulnerable to attack and that some degree of government intervention in the private sector is necessary).

[169] Cyber Security Public Awareness Act of 2011, S. 813, 112th Cong. § 3(a)(1) (2011).

[170] *Id.* § 3(b)(1).

[171] *Id.* § 12.

[172] *Id.* § 11.

[173] *Id.* § 7.

[174] *Id.* § 4(a)(1).

[175] *Id.* § 6.

[176] *Id.* § 5(a). The term *information network* is conspicuously left undefined in the bill.

[177] *Id.* § 8.

[178] *Id.* § 10.

[179] Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. sec. 2(a), § 222(a)(1) (2011).

gence community Federal systems" via an "interagency working group" comprising top technology officials from "all Federal civilian agencies."[180] OCC's new Cybersecurity Compliance Division would be responsible for working with relevant regulatory agencies (e.g., the Department of Energy for power plants) to develop and implement cybersecurity regulations through a typical notice-and-comment rulemaking process.[181]

HSCPIPA is the first of the bills to go beyond regulating government networks, extending OCC's regulatory authority to "private sector computer networks within covered critical infrastructures."[182] OCC itself would decide what counts as "covered critical infrastructures," based on a consideration of the "national information infrastructure"; the likelihood of "a national or regional catastrophe" should the covered system be destroyed; known security risks; infrastructure interdependency; and the possibility of "mass casualty event[s]," "severe economic consequences," "mass evacuations," or "severe degradation of national security capabilities" occurring.[183] Owners of private systems designated as critical could appeal OCC's decision (through a method to be determined by OCC), but barring a reversal of that determination, they would be required to submit "cybersecurity plans" to the appropriate supervising agency for review and approval.[184] Noncompliance would subject companies to civil penalties of up to $100,000 per day per instance.[185]

The legislation's scope expands further, requiring information sharing among regulated entities[186] and providing for vague protections of "sensitive security information" obtained through the regulatory process.[187] Rounding out HSCPIPA are provisions recognizing a commitment to research and development[188] and annual agency audits of workforce needs, focusing on the recruitment and retention of cybersecurity specialists.[189]

7. *Executive Cyberspace Coordination Act of 2011*.—A similar take on comprehensive cybersecurity legislation is offered by the Executive Cyberspace Coordination Act of 2011 (ECCA).[190] In order to "provide a comprehensive framework" for federal information security,[191] ECCA would

[180] *Id.* sec. 2(a), § 223(a)–(b)(1). The OCC would also be responsible for oversight and enforcement. *Id.* sec. 2(a), § 223(d)–(f).

[181] *Id.* sec. 2(a), § 223(b)(1), (3).

[182] *Id.* sec. 2(a), § 224(b).

[183] *Id.* sec. 2(a), § 224(e)(1)–(3).

[184] *Id.* sec. 2(a), § 224(e)(4)–(g).

[185] *Id.* sec. 2(a), § 224(m).

[186] *Id.* sec. 3.

[187] *Id.* sec. 4.

[188] *Id.* sec. 5.

[189] *Id.* sec. 6.

[190] Executive Cyberspace Coordination Act of 2011, H.R. 1136, 112th Cong. (2011).

[191] *Id.* sec. 101, § 3551(1).

create the National Office for Cyberspace within the Executive Office of the President.[192] Headed by a presidentially appointed and Senate-confirmed director[193] who would preside over the interagency Federal Cybersecurity Practice Board,[194] the National Office for Cyberspace would periodically promulgate government-wide cybersecurity policies and standards.[195] Much like HSCPIPA,[196] this bill would burden the individual government agencies with developing and implementing programs to accomplish the goals set forth by the new office.[197] Agencies would also be tasked with auditing their cybersecurity programs and practices each year.[198]

Adding a layer of confusion to the new regulatory bureaucracy, the Secretary of Commerce would be granted power to issue compulsory, binding standards to enhance the security of federal information systems.[199] Additionally, the bill mandates the creation of an information clearinghouse for collecting and analyzing data on security incidents[200] and an Office of the Federal Chief Technology Officer.[201]

ECCA also recognizes the need to enhance private-sector security and would authorize broad regulation of privately owned systems via an expansive definition of "critical information infrastructure."[202] If all "electronic information and communications systems, software, and assets that control, protect, process, transmit, receive, program, or store information in any form . . . relied upon by critical infrastructure" are covered, it is difficult to imagine what would not be considered critical.[203]

8. Cybersecurity and Internet Freedom Act of 2011.—The Cybersecurity and Internet Freedom Act of 2011 (CIFA)[204] is the most storied of the proposals before the 112th Congress. It was originally

[192] *Id.* sec. 101, § 3553(a).

[193] *Id.* sec. 101, § 3553(b).

[194] *Id.* sec. 101, § 3554.

[195] *Id.* sec. 101, § 3554(c)–(d).

[196] *See supra* section IV(C)(6).

[197] *See* H.R. 1136 sec. 101, § 3556(b).

[198] *Id.* sec. 101, § 3557.

[199] *Id.* sec. 101, § 3558.

[200] *Id.* sec. 101, § 3559.

[201] *Id.* sec. 201(a)(1)(A); *see also supra* section IV(C)(4).

[202] H.R. 1136 sec. 301(1).

[203] *Id.*; *see also* PJ Coyle, *HR 1136 Introduced—Cyber Security*, CHEMICAL FACILITY SECURITY NEWS (Mar. 19, 2011, 3:08 PM), http://chemical-facility-security-news.blogspot.com/2011/03/hr-1136-introduced-cyber-security.html ("Taken to its logical extreme, this definition would include the electronics system in every modern automobile. . . . The only saving grace is that the scope and authority is so wide and all encompassing as to be practically meaningless. Any attempt to establish cybersecurity regulations under this authority would be tied up in court so fast that thousands of lawyers would get rich on the billable hours on these cases alone.").

[204] Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011). At 221 pages, the CIFA is a daunting piece of legislation. A complete analysis of the bill is therefore beyond the scope of this Note, although most of the highlights are discussed.

proposed in June 2010 under a different name: the Protecting Cyberspace as a National Asset Act of 2010 (PCNAA).[205] PCNAA would have granted the President the power to declare a "national cyber emergency,"[206] which would have enabled a newly formed government agency to force owners and operators of critical infrastructure into immediate compliance with "any emergency measure or action."[207] Those sweeping provisions led the media to widely pan the bill as an Internet kill switch,[208] though its primary sponsor, Senator Joseph Lieberman, repeatedly came to its defense.[209] Public outcry intensified when it was revealed that a committee revision of the bill immunized from judicial review the government's decision to classify privately owned systems as critical.[210] The bill never saw a vote on the Senate floor.[211]

In 2011, the PCNAA reemerged in Congress, modified in a number of ways and sporting a new user-friendly nickname promoting "Internet Freedom."[212] CIFA would create the Office of Cyberspace Policy within the Executive Office of the President, and charge the new office with developing "a national strategy to increase the security and resiliency of cyberspace."[213] That multifaceted strategy would encompass everything from "computer network operations" and "protection of critical infrastructure" to "diplomacy" and "military and intelligence activities."[214] To retain some

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

[206] *Id.* sec. 201, § 249(a)(1).

[207] *Id.* sec. 201, § 249(c)(1).

[208] *See, e.g.*, Albanesius, *supra* note 6 (recounting that the controversy swirling around the bill "prompted many to dub [the] option an 'Internet kill switch'"); Jon Orlin, *In Search of the Internet Kill Switch*, TECH CRUNCH (Mar. 6, 2011), http://techcrunch.com/2011/03/06/in-search-of-the-internet-kill-switch/ ("It became known as the Internet 'kill switch' bill even though the words 'kill' and 'switch' are not found in the bill."); Matthew Schafer, *How the Internet "Kill Switch" Bill Became the Bulwark of Internet Independence*, GROUND REP. (Feb. 21, 2011), http://www.groundreport.com/Business/How-the-Internet-Kill-Switch-Bill-Became-the-Bulwa/2934942 (noting that the bill was "subject to a maelstrom of controversy" after being dubbed a kill switch); *see also* Declan McCullagh, *Senators Propose Granting President Emergency Internet Power*, CNET NEWS (June 10, 2010), http://news.cnet.com/8301-13578_3-20007418-38.html (recognizing "few limits on the president's emergency power, which can be renewed indefinitely," and noting industry concerns over "the potential for absolute power").

[209] *See, e.g.*, Albanesius, *supra* note 6 ("Right now, China, the government, can disconnect parts of its Internet in a case of war. We need to have that here, too . . . ." (quoting Sen. Lieberman)); Orlin, *supra* note 208 ("Lieberman generously suggested the president is 'not going to do it every day' (phew), but he did argue 'we need the capacity for the president to say, Internet service provider, we've got to disconnect the American Internet from all traffic coming in from another foreign country, or we've got to put a patch on this part of it.'").

[210] *See, e.g.*, Declan McCullagh, *Internet "Kill Switch" Bill Will Return*, CNET NEWS (Jan. 24, 2011), http://news.cnet.com/8301-31921_3-20029282-281.html ("The revised version includes new language saying that the federal government's designation of vital Internet or other computer systems 'shall not be subject to judicial review.'").

[211] Chloe Albanesius, *After Egypt, Will U.S. Get "Internet Kill Switch"?*, PC MAG (Jan. 28, 2011), http://www.pcmag.com/article2/0,2817,2376888,00.asp.

[212] Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. sec. 1 (2011).

[213] *Id.* sec. 101(a)(1).

[214] *Id.*

control over the direction of the Office of Cyberspace Policy, the Senate would reserve the right to confirm the President's choice for the Office's head role.[215]

Further congressional oversight would come in the form of a new Department of Homeland Security subunit, the National Center for Cybersecurity and Communications (NCCC).[216] While there would be overlap in the duties of the two new offices,[217] it appears that Congress envisions a larger role for NCCC.[218] Federal regulation comes standard, and private-sector regulation reappears through CIFA's definition of "critical infrastructure,"[219] which is largely similar to the measured and systematic approach taken by the HSCPIPA.[220] CIFA also contains the oft-seen provisions calling for information sharing;[221] private-sector assistance;[222] employment, education and professional development;[223] and expanded research and development efforts.[224]

While the new version of CIFA preserves the presidential emergency-power provisions of its predecessor,[225] an expanded list of disclaimers appears to limit the most egregious exercises of power[226] and the duration of the emergency.[227] The drafters pay lip service to earlier critics with a provision noting that neither CIFA nor the Communications Act of 1934 provides "authority to shut down the Internet."[228] The ultimate effect of such a vague disavowal of power remains the subject of some debate.[229]

[215] *Id.* sec. 102(a)(1).

[216] *Id.* sec. 201, § 242. NCCC would also be headed by a presidentially appointed, Senate-confirmed director. *Id.* sec. 201, § 242(b)(1).

[217] *Compare id.* sec. 102(b) (outlining the duties of the director of OCP), *with id.* sec. 201, § 242(f) (outlining the duties of the director of NCCC).

[218] *See id.* sec. 201, § 242(f)(1)(A) (calling upon the NCCC director to "lead the Federal effort to secure, protect, and ensure the resiliency of the Federal information infrastructure, national information infrastructure, and communications infrastructure of the United States").

[219] *Id.* sec. 201, § 248(a)(2).

[220] *See supra* section IV(C)(6).

[221] *Id.* sec. 201, § 246.

[222] *Id.* sec. 201, § 247.

[223] *Id.* secs. 401–408.

[224] *Id.* sec. 501.

[225] *Id.* sec. 201, § 249; *supra* notes 206–07 and accompanying text.

[226] *See, e.g.*, S. 413 sec. 201, § 249(a)(6)(B) (prohibiting the government from outright "control[ling] covered critical infrastructure").

[227] *See id.* sec. 201, § 249(b) (limiting the effect of a "national cyber emergency" to thirty days from the date of a presidential declaration, with limited exceptions).

[228] *Id.* sec. 2(c).

[229] *See* Editorial, *The Internet Kill Switch Rebooted*, WASH. TIMES, Mar. 7, 2010, *available at* http://www.washingtontimes.com/news/2011/mar/7/the-internet-kill-switch-rebooted/ ("Dumb ideas never die in Washington; they're just re-invented. . . . [CIFA] still gives the White House authority to declare a vaguely defined 'cyber emergency' that empowers bureaucrats to issue directives to Internet companies with which they must 'immediately comply.'"); *Senators Re-introduce Cybersecurity Bill, with Key Difference*, INFOSECURITY (Feb. 22, 2011), http://www.infosecurity-

V. A New Framework

With no shortage of solutions available for addressing the cybersecurity issue, the difficulty lies in choosing the best one. Many of the proposals discussed in Part IV offer insightful, realistic solutions; others are ineffectual or go too far. The final portion of this Note sketches a broad framework for protecting America's networks, drawing upon ideas from a variety of sources. While this framework lacks the depth and specificity needed for immediate implementation, it nevertheless offers a jumping-off point for a unified and comprehensive approach to national cybersecurity.

A. The Locus of Control

The first question for any cybersecurity solution concerns where to concentrate the power to implement whatever new policies are developed. The White House has recently sought to vest cybersecurity power within the Executive Branch and away from the control of Congress.[230] Several of the proposals currently before Congress take a more traditional approach, requiring Senate confirmation of new top cybersecurity officials.[231] The congressional appointment process and accompanying oversight offer significant benefits to the development of a stable and transparent cybersecurity policy; thus, locating power within the Legislative Branch is the better solution.

An initial benefit to constitutionally appointed officers like department secretaries is the extensive vetting process that seeks to ensure that the best candidate for a particular position is chosen.[232] Senate confirmation is often the only hurdle that stands between the unqualified masses and a high-ranking job within the United States government.[233] Though the vetting process has been criticized for becoming "drawn-out and often disagreeable,"[234] it remains preferable to the alternative: the creation of additional White House "czars."

us.com/view/16119/senators-reintroduce-cybersecurity-bill-with-key-difference/ ("Privacy advocates are still concerned about the power given to the president in the bill.").

[230] Pearlman, *supra* note 147, at 4.

[231] *See supra* notes 193, 215 and accompanying text.

[232] For example, a number of recent appointees saw their appointments derailed during the vetting process when concerns surfaced over their personal employment of undocumented workers. David E. Sanger, *Nominee's Quick Exit Not a First for Bush*, N.Y. TIMES, Dec. 12, 2004, at N48.

[233] *See* G. Calvin Mackenzie, *The State of the Presidential Appointments Process, in* INNOCENT UNTIL NOMINATED: THE BREAKDOWN OF THE PRESIDENTIAL APPOINTMENTS PROCESS 1, 2 (G. Calvin Mackenzie ed., 2001) ("When a new American president takes office, he is permitted to fill thousands of executive branch positions with people whose only necessary qualification is their ability to endure and survive the Senate confirmation process. Like him, they need bring no experience in national government nor even any demonstrable acquaintance with the department or agency in which they will serve.").

[234] George P. Shultz, Op.-Ed., *The Constitution Doesn't Mention Czars*, WALL ST. J., Apr. 11, 2011, *available at* http://online.wsj.com/article/SB10001424052748703806304576234724010496418.html; *see also id.* (noting that the vetting

Czars are members of the White House staff "with de facto decision-making power" in a selected area.[235] Presidential administrations since Franklin Roosevelt's have varied in their use and appointment of czars.[236] The Obama administration has dozens of czars with authority in a variety of areas,[237] including current "cyberczar" Howard Schmidt, the White House Cybersecurity Coordinator.[238] In addition to the constitutional questions raised by the selection of White House czars,[239] the czars themselves are unaccountable and often formulate bad policies because they lack the institutional knowledge and expertise built into the cabinet-government structure.[240]

Whatever form the new cybersecurity bureaucracy takes, the government should use the reshuffling as an opportunity to consolidate leadership on the issue going forward.[241] Currently, in addition to Obama's cyberczar, the Department of Homeland Security's Office of Cybersecurity and Communications is charged with tackling cybersecurity issues.[242] The White House Office of E-Government and Information Technology lists cybersecurity among its "key initiatives,"[243] and the National Security Council has a Cybersecurity Office that coordinates with the Federal Chief

process may discourage talented people from seeking office); Alexander Mooney, *Obama's Vetting Could Chase Away Candidates*, CNN POLITICS (Nov. 22, 2008), http://articles.cnn.com/2008-11-22/politics/obama.vetting_1_longtime-obama-supporter-obama-transition-choice-for-commerce-secretary (same).

[235] Shultz, *supra* note 234; *see also tsar | czar, n.*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/viewdictionaryentry/Entry/207078 (draft addition) ("A person appointed by a government to recommend and coordinate policy in a particular area and to oversee its implementation. Usually with modifying word denoting the area of responsibility.").

[236] Jonathan D. Puvak, Note, *Executive Branch Czars, Who Are They? Are They Needed? Can Congress Do Anything About Them?*, 19 WM. & MARY BILL RTS. J. 1091, 1095–98 (2011).

[237] *Id.* at 1098–99.

[238] Editorial, *Obama's Smart Pick for Cyber Czar: Howard Schmidt*, CHRISTIAN SCI. MONITOR (Dec. 23, 2009), http://www.csmonitor.com/Commentary/the-monitors-view/2009/1223/Obama-s-smart-pick-for-cyber-czar-Howard-Schmidt.

[239] *See* Puvak, *supra* note 236, at 1108–12 (examining the constitutionality of czar appointments under the Appointments Clause).

[240] Shultz, *supra* note 234. George Shultz, a former Secretary of State under President Reagan, cites the Iran-Contra scandal as a "dramatic example" of the consequences of vesting too much power in White House staffers. *Id.*

[241] *See* Editorial, *supra* note 229 (bemoaning the current cybersecurity bureaucracy for inspiring "more interagency meetings and the production of additional reports and memos nobody will read").

[242] *Office of Cybersecurity and Communications*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm (last modified Aug. 19, 2011).

[243] *Office of E-Government & Information Technology*, WHITE HOUSE, http://www.whitehouse.gov/omb/e-gov/.

Technology Officer on cybersecurity issues.[244] The various proposals before Congress[245] seek to add additional layers to this complex bureaucratic tower.

Instead of creating yet another quasi-regulatory body to offer opinions, the new cybersecurity landscape should be streamlined, consolidating expertise and power in a central location. Federal cybersecurity policy must be uniform and come from above. A top-down structure eliminates the problems inherent in asking individual agencies to develop their own security strategies. After all, the lack of uniformity, consistency, and compatibility is already a leading contributor to cybersecurity risks.[246]

B. Safeguarding Internet Availability

"The Internet is vital to almost every facet of Americans' daily lives . . . ."[247] Access to the Internet is synonymous with the ability to communicate, stay informed, and engage in the myriad daily tasks that Internet users—from the casual individual to highly sophisticated corporations—find necessary.[248] America's new cybersecurity framework must not contain the current "broad and ambiguous" powers of the government to shut the Internet down in times of emergency.[249] Vague disavowals of power, like the one contained in CIFA,[250] do not go far enough. The Communications Act of 1934 should be expressly modified to cabin the President's emergency powers.[251] While Internet access need not become a new basic human right,[252] the ability of the government to deny Americans access to such a crucial communications medium must be explicitly outlined,

[244] *Cybersecurity*, WHITE HOUSE, http://www.whitehouse.gov/administration/eop/nsc/cybersecurity. It is this office that is charged with implementing the CNCI. *See supra* notes 147–52 and accompanying text.

[245] *See supra* subpart IV(C).

[246] *See, e.g.*, S. REP. NO. 111-368, at 14 (2010) (noting that the current "fragmented leadership" makes it difficult to "recruit and retain highly skilled cyber experts"); CYBERSPACE POLICY REVIEW, *supra* note 47, at i ("Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way.").

[247] 157 CONG. REC. S910 (daily ed., Feb. 17, 2011) (statement of Sen. Collins).

[248] *See id.* ("It is essential that the Internet and our access to it be protected to ensure both reliability of the critical services that rely upon it and the availability of the information that travels over it."); s*ee also* Pew Research Center, *Daily Internet Activities, 2000–2009*, PEW INTERNET, http://www.pewinternet.org/Trend-Data/Daily-Internet-Activities-20002009.aspx (cataloguing the various daily Internet activities of American adults).

[249] *See supra* note 125 and accompanying text.

[250] *See supra* notes 228–29 and accompanying text.

[251] *See* Reitinger Testimony, *supra* note 124 (advocating modifications to the Communications Act of 1934 in lieu of creating new emergency-power legislation).

[252] Several countries have made Internet access a basic right. *E.g.*, *First Nation Makes Broadband Access a Legal Right*, CNN (July 1, 2010), http://articles.cnn.com/2010-07-01/tech/finland.broadband_1_broadband-access-internet-access-universal-service (Finland); *Spain Govt to Guarantee Legal Right to Broadband*, REUTERS (Nov. 17, 2009), http://www.reuters.com/article/2009/11/17/spain-telecoms-idUSLH61554320091117 (Spain).

carefully tailored, and subject to the traditional checks and balances of democratic governance.

C. Regulation

The most controversial aspect of a new cybersecurity scheme is bound to be the nature and extent of governmental regulation. Because government networks and private networks differ in a number of ways, unique solutions must be crafted to address the concerns raised by each breed.

1. Securing Government Networks.—Returning to a common theme, consistency and uniformity are the key attributes of cybersecurity solutions aimed at government-controlled networks. Many of the proffered legislative responses task each agency with creating and implementing its own cybersecurity policy, sometimes subject to approval by a top official.[253] The inevitable result of agency-specific solutions is a proverbial patchwork quilt, an indecipherable web of different protective measures with no unified plan or even a single technical body capable of quickly making sense of America's cybersecurity strengths and weaknesses.

Consistency is the solution to this problem. For example, imagine the simplicity and strength of a uniform federal authentication system designed to verify, track, and control access to different portions of the federal network structure based on a standard security scheme.[254] Additionally, if federal networks were standardized, fixing security holes would be significantly easier. Rather than sifting through each agency's unique cybersecurity structure to determine where a leak occurred and how to patch it, the government could diagnose and treat security holes in a unified system in a fraction of the time. Many of the most crippling security issues are solved long before they ever become problematic, but because systems are not uniformly updated, weak links in the chain become easy targets.[255]

In securing the nation's governmental networks, the government should also leverage its significant buying power to influence product development

[253] *See, e.g.*, Executive Cyberspace Coordination Act of 2011, H.R. 1136, 112th Cong. sec. 101, § 3556(b) (2011) (as referred to H. Subcomm. on Cybersecurity, Infrastructure Protection, & Sec. Techs., Mar. 25, 2011) ("Each agency shall develop, document, and implement an agencywide information security program, approved by the Director of the National Office for Cyberspace . . . .").

[254] *See* 2003 NATIONAL STRATEGY, *supra* note 140, at 46 (noting the difficulties inherent in the government's current, inadequate authentication system and emphasizing the need to "promote consistency and interoperability").

[255] For example, the vulnerability exploited by the SQL Slammer had been addressed months before the worm was created. *See supra* note 65 and accompanying text. Even novel "zero-day" exploits are often patched within hours of their discovery. *See, e.g.*, Richmond, *supra* note 89. But solutions are worthless if systems are never updated—a constant risk facing agency-specific security solutions that makes verification, enforcement, and monitoring of such compliance measures difficult.

in the cybersecurity market.[256] By demanding more of private contractors who supply government agencies with security necessities like hardware and software, the government can encourage innovation that benefits federal networks and ultimately spills over to the consumer marketplace.[257] Government information is some of the most sensitive data in digital form, and the government's cybersecurity solutions should reflect that sensitivity by employing the most robust and up-to-date systems available.

2. Securing Private Networks.—Protecting government systems from attack is only half of the solution. The private sector is equally vulnerable, as the SQL Slammer and the recent attacks against Google illustrate. Some degree of government intervention in the private sector is necessary because the traditional laissez-faire approach of deferring to market forces has proven to be inadequate.[258] The problem is particularly troublesome when dealing with utility providers (like electric companies) whose market and product positioning make them less likely to lose customers as a result of security breaches than services like those provided by Google or Sony.[259]

One solution to the private-sector problem is the use of so-called smart regulation, which specifies goals rather than methods.[260] While smart regulation provides the flexibility the private sector needs,[261] it nevertheless must be backed by some sort of enforcement mechanism or it risks becoming meaningless.[262] HSCPIPA, which would empower the Department of Homeland Security to levy civil fines of up to $100,000 per day on

[256] *See* CSIS REPORT, *supra* note 25, at 13 ("The metric for success is straightforward: federal acquisitions require government agencies to buy more secure products or services.").

[257] *See id.* ("Government purchases of new security solutions will both drive down the cost of those solutions and serve as a proving ground for their effectiveness."); *see also* Paller Testimony, *supra* note 111, at 94 ("[O]nly massive procurement power can persuade vendors to deliver safer systems rather than the standard systems they sell at retail to businesses and consumers.").

[258] *See* CSIS REPORT, *supra* note 25, at 7 ("[N]ational security and public safety always require more than the market can deliver. The September 2010 Stuxnet incident . . . is a harbinger of what is to come. The market will not deliver adequate security in a reasonable period, and voluntary efforts will be inadequate against advanced nation-state opponents."); TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 303–04 (2010) (arguing that "the purely economic laissez-faire approach . . . is no longer feasible" when dealing with the information industry).

[259] Of course, market forces such as the possibility of losing customers are no guarantee of proper security. In April 2011, Sony's popular online gaming service, the PlayStation Network, was hacked, spilling the personal information of its seventy million users into the hands of the attackers. Jason Schreier, *PlayStation Network Hack Leaves Credit Card Info at Risk*, WIRED (Apr. 26, 2011), http://www.wired.com/gamelife/2011/04/playstation-network-hacked/.

[260] *See* CLARKE & KNAKE, *supra* note 56, at 132 (indicating that a majority of cybersecurity experts favor a limited amount of smart regulation).

[261] *See* CSIS REPORT, *supra* note 25, at 7 (advocating minimally burdensome, "flexible rather than prescriptive," regulation).

[262] *See Cyber Security: Developing a National Strategy: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. 84–85 (2009) (statement of Hon. Stewart A. Baker, Former Assistant Secretary of Homeland Security) (cautioning against overly flexible, procedural approaches that lack specific security requirements).

noncompliant critical infrastructure owners, is an example of a proposal with serious teeth.[263] Of course, the potential to levy fines is worthless (and will not encourage compliance) if it is never used.[264]

Enforceable, flexible regulations are valuable, but they must be implemented judiciously to avoid overburdening both regulators and private-sector entities. Private-sector regulation should, at least initially, be limited to a narrower category of networks than the current legislative proposals cover with their sweeping definitions of "critical infrastructure."[265] Significant improvements to cybersecurity could be achieved by limited regulation of two key areas: utility networks and tier-one ISPs.

Utility networks include industries like power generation and water distribution, core services the nation depends on to remain functioning. At least until these industries prove that they are capable of securing their networks, a simple solution is to disconnect such critical systems from the Internet entirely.[266] The security industry refers to this process as creating an "air gap" between supercritical systems and the general network.[267] Air gaps may be somewhat burdensome, but the security payoff is unparalleled: air-gapped systems are fully isolated and practically impervious unless an attacker manages to physically access the system.

Tier-one ISPs are the second piece of the puzzle. The handful of companies that make up tier one form the "backbone of the Internet," effectively controlling over 90% of Internet traffic within the United States.[268] Simply put, "it is usually impossible to get to anyplace in the U.S. without traversing one of these backbone providers."[269] Smart regulation of tier-one ISPs could secure the gateway to virtually every major national network. The use of "deep-packet inspection," a process that analyzes each individual piece of information flowing across a network,[270] could provide the ISPs with the ability to detect and cut off malicious traffic (like a DDoS attack) before it becomes problematic. Proper oversight could allay privacy concerns,[271] and the flexible nature of smart regulation would allow for further protections to be implemented as needed.

[263] *See supra* note 185 and accompanying text.

[264] *See* CLARKE & KNAKE, *supra* note 56, at 168 (explaining the difficulties of enforcing cybersecurity regulations in the absence of publicly available standards).

[265] *See, e.g.*, *supra* notes 202–03 and accompanying text.

[266] *See* CLARKE & KNAKE, *supra* note 56, at 132 (noting that "[t]he idea of separating 'critical infrastructure' from the open-to-anyone Internet seemed pretty obvious to the seasoned group of information security specialists" gathered at the 2009 Black Hat security conference).

[267] Oliver Rist, *Hack Tales: Air-gap Networking for the Price of a Pair of Sneakers*, INFOWORLD (May 29, 2006), http://www.infoworld.com/d/networking/hack-tales-air-gap-networking-price-pair-sneakers-610. The term is derived from the fact that there is "nothing but air" between the two networks. *Id.*

[268] CLARKE & KNAKE, *supra* note 56, at 160.

[269] *Id.*

[270] *Id.* at 161–62.

[271] *Id.* at 162.

D. Long-Term Investments

The final component in the new cybersecurity framework is a long-term commitment to the cybersecurity issue. Returning to the days of ARPA and the creation of the Internet, the government must seriously (re)invest in the Internet security field.[272] The proposals before Congress focusing on education, job training and recruitment, and scientific investment are on the right track. There should also be room within the cybersecurity bureaucracy for an official team of government "white-hat" hackers, technological experts who opt to use their knowledge and skills to improve the security of information systems by finding vulnerabilities and pointing them out to the owners of the networks.[273] Naturally, government sponsorship and control over this white-hat team would necessitate the creation of exemptions (official or unofficial) for team members from laws like the Computer Fraud and Abuse Act that outlaw a variety of hacking-related activities.[274]

VI. Conclusion

"[C]ybersecurity is now a major national security problem for the United States . . . ."[275] Despite an abundance of evidence that the problems are both vast and significant, the current debate has become "stuck."[276] This Note attempts to move the discussion forward by proposing a comprehensive new framework that eschews several ideas of the old guard[277] in favor of bold new solutions. Recent events in Egypt and elsewhere around the globe have set the stage for a cybersecurity revolution. That momentum should be harnessed and used to enact legitimate and effective reform to secure the future of the Internet and everything it touches.

—Karson K. Thompson

[272] *See id.* at 131–32 (reporting consensus among the Black Hat group of cybersecurity experts that the Bush Administration's virtual abandonment of cybersecurity research and development was a mistake).

[273] For a description of white-hat hacking and its potential role in national and international cybersecurity, see *What Is a White Hat*, SECPOINT, http://www.secpoint.com/What-is-a-White-Hat.html (explaining how white-hat hackers use their talents to help improve network security and pointing out that the National Security Agency even offers white-hat certification).

[274] *See* 18 U.S.C. § 1030 (2006) (outlining, among other things, computer-security-related offenses and punishments).

[275] CSIS REPORT, *supra* note 25, at 15.

[276] *Id.* There appears to be a widespread belief among policymakers that "we [as a nation] will be unable to take any meaningful action on cybersecurity until after some large and damaging event." *Id.*

[277] "Many of the solutions still advocated for cybersecurity are well past their sell-by date." *Id.* In particular, ideas like self-regulation "are remedies we have tried for more than a decade without success." *Id.*