American University National Security Law Brief

Volume 1 | Issue 1 Article 8

2011

Cybersecurity: Domestic and Legislative Issues

Sean Shank

CYBERSECURITY: DOMESTIC AND LEGISLATIVE ISSUES

Sean Shank*

Despite the prominence of the health care and stimulus debates throughout the first years of the Obama administration, political affairs in Washington, D.C. have quietly yielded major developments in efforts to secure cyberspace. Exercises by the Bipartisan Policy Center,[1] the establishment and appointment of a new cybersecurity coordinator for the White House,[2] and pending legislation[3] indicate that cyber security issues comprise an area of growing concern. Some experts, including former Director of National Intelligence J. Michael McConnell, view American electronic infrastructure as an area ripe for exploitation by terrorists,[4] while other experts rightly indicate that such infrastructure is already subject to exploitation.[5] Attempting to address this concern, various bills, especially the Senate Homeland Security Committee's "Protecting Cyberspace as a National Asset Act"

* Sean Shank is a 2011 JD/MA candidate at American University – Washington College of Law. For his joint degree program he is concentrating on national security law, cybersecurity, and nuclear non-proliferation. He earned an A.B. from Princeton University in East Asian Studies and is fluent in Japanese.

1 *See Cyber ShockWave Shows U.S. Unprepared For Cyber Threats*, Bipartisan Policy Center, Feb. 17, 2010, [hereinafter *Cyber ShockWave*] *available at* http://www.bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats (discussing the potential weaknesses of a government counterterror response based on a simulated cyberattack).

2 *See* Macon Phillips, *Introducing the New Cybersecurity Coordinator*, The White House Blog (December 22, 2009, 7:30 AM), http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator (announcing Howard Schmidt's selection as White House Cybersecurity Coordinator).

3 *See* Eric Chabrow, *Infosec Provisions Seen as Rider to Senate Defense Bill,* GovInfo Security, August 25, 2010, *available at* http://www.govinfosecurity.com/articles.php?art_id=2868 (describing potential efforts to attach cybersecurity legislation to the National Defense Authorization Act, as well as efforts by Senate leadership to combine various competing cybersecurity bills into one omnibus bill).

4 *See* Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, Wash. Post, February 28, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html? sid=ST2010031901063 (discussing insufficient protection for, *inter alia*, power grids, transportation, and telecommunications networks).

5 *See, e.g.* Siobhan Gorman, *Grid is Vulnerable to Cyber-Attacks*, Wall St. J., August 3, 2010, *available at* http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704905004575405741051458382.html (indicating the threat from ongoing Russian and Chinese electronic surveillance of U.S. energy grid).

(PCNAA)[6], have inflamed concerns about granting the White House internet "kill switch" authority.[7] Broadly stated, this authority would give the White House the ability to shut off parts of the internet subjected to sophisticated hacking, distributed denial-of-service (DDoS)[8], or other attacks.

These concerns warrant a number of questions, including: would an internet kill switch pose a threat to private enterprise or civil liberties? If legislation did, in fact, provide the President with the ability to "shut off" the internet, does this accord with his legal and constitutional authority?[9] Even if this authority passes constitutional muster, is a kill switch technically sound?[10] Bills such as PCNAA and Senator Jay Rockefeller's Cybersecurity Act of 2010 (introduced in 2009)[11] assign the White House and other Executive Branch agencies with new responsibilities that attempt to address such technical concerns by granting the White House considerable emergency authority in monitoring and operating the internet. The Rockefeller Bill would convert the Department of Commerce into a clearing-house of industry network security information[12], while under PCNAA, the White House and the Department of Homeland Security (DHS) would have considerable power over the internet in the event of an emergency. Private business would be required to abide by emergency executive orders upon an indication that an emergency existed.[13]

Even if the White House has the legal authority for a kill switch operation, the viability of such a measure could actually be more of a technical problem than a Constitutional one. If the United States' critical infrastructure were subjected to a devastating cyberattack, it might be reasonable to grant the President aggressive authority to commandeerU.S. networks. It is now a truism that the Executive Branch's war and national security powers have expanded in the wake of 9/11 — for such power to be available in the arena of cybersecurity is neither surprising nor inappropriate. Perhaps it is even *less* surprising, given the concern that a continually vulnerable electronic infrastructure could serve as the staging ground for the next 9/11. Due to the growing sophistication of certain hackers, attribution is difficult, and routine internet use can result in unwittingly exposing one's computer to

---

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

7 *See* Adam Cohen, *What's Missing in the Internet Kill-Switch Debate*, TIME MAGAZINE, August 11, 2010*, available at* http://www.time.com/time/nation/article/0,8599,2009758,00.html?xid=rss-mostpopular (describing ideologically diverse opposition to enhanced White House control over the internet for security purposes).

8 A DDoS attack is one in which a master computer may control a botnet, or series of compromised computers, to direct inordinate amounts of traffic to a website so as to make it unavailable.

9 In addition to the Executive Branch's constitutional authority, some commentators indicate that the Communications act of 1934 also provides the White House with the authority it would need to control the internet in the event of an emergency. *See id.* (indicating that the President "already has broad power under the Communications Act of 1934 to shut down wire communications . . . includ[ing] the internet"); *see also* Communications Act of 1934 (codified at 47 U.S.C.S. § 606(d)(2) (LexisNexis 2010)) (granting the President the authority to "cause the closing of any facility or station for wire communication and the removal therefrom of its apparatus and equipment").

10 *See The Fear-Based Psychology of the 'Internet Kill Switch,'* TECHNOLOGY REVIEW, August 18, 2010, *available at* http://www.technologyreview.com/blog/mimssbits/25628/ (in which interviewee Paul Kocher describes the kill switch as a "blunt weapon" and questions the benefit of its implementation).

11 Cybersecurity Act of 2010, S.773, 111th Cong. (2009).

12 *Id.* § 14(a) (referring to private sector network vulnerabilities).

13 S. 3480 § 249(a)(1).

an unlawful botnet.[14] In short, the risks are many, but combating them through legislation must be carried out with an eye for technical limitations.

Cybersecurity Abroad: Challenges, Conflicts, and a Need for Legal Norms

When viewed in an international legal context, the term "cybersecurity" may suggest a broader, more inchoate meaning. "Cybersecurity" not only encompasses matters involving DDoS attacks from isolated hackers, but can also include emerging aspects of state-to-state warfare, as well as questions about whether access to electronic information should be deemed a human right.[15] In certain contexts, U.S. foreign policy reflects an intersection of security and human rights concerns — while members of the legislature cite to the cyber-threat posed by China[16], members of the Executive Branch laud U.S. efforts to disrupt authoritarian controls on internet activities by human rights activists.[17] There are many threats that warrant U.S. involvement, even if international law does not always provide sufficient guidance in all contexts.

In its summer 2008 conflict with Georgia, Russia accompanied its military incursions with cyberattacks on Georgian computer systems.[18] Russian state hackers, and independent hackers within Russia have long been suspected as sources of other cyberattacks against foreign states, including the crippling 2007 DDoS attacks against Estonia. These attacks against "eStonia" (nicknamed for its well-developed domestic internet access[19]) continued for over a month as an extended "cyber-riot," threatening Estonian electronic infrastructure, including its banking system.[20] However, unlike the 2008 attacks on Georgian computer networks, it is unclear how responsible the Russian government, or any other party, was for the 2007 "Web War I" against Estonia. Even for analysts and agencies that have robust resources, attribution is a technological problem — making legal determination of state responsibility even *more* difficult.[21]

China is a prominent example of how freedom of access to information, cybersecurity, and

---

14 *See FTC Consumer Alert: Botnets and Hackers and Spam (Oh, My!)*, F. T. C., June 2007, *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt132.shtm.

15 *See* Hillary Clinton, Secretary of State, Remarks on Internet Freedom at Newseum, (January 21, 2010) (transcript *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm) (discussing a "universal right to come together with those who share your values . . .").

16 *See* Chloe Albanesius, *Lieberman Backs Away from 'Internet Kill Switch'*, PCMag.com, June 21, 2010, http://www.pcmag.com/article2/0,2817,2365393,00.asp.

17 *See* Clinton *supra* note 15.

18 Kevin Coleman, *Cyber War 2.0 – Russia v. Georgia*, Defense Tech, *available at* http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia.

19 90% of Estonia's banking, at a minimum, is internet-based. Elections are also conducted via the internet. *See* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, Wired Magazine, August 21, 2007, *available at* http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

20 *See* Shaun Waterman, *Analysis: Who Cyber Smacked Estonia?*, United Press International, June 11, 2007, *available at* http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/ (describing Professor James Hendler's characterization of the attacks as more of a "cyber riot").

21 *See* Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,* 27 Berkeley J. Int'l L. 192, 231–36 (2009).

American foreign policy are entangled. In a January 2010 speech, Secretary of State Hillary Clinton praised U.S. efforts to assist human rights dissidents in China with their bypass of network restrictions put in place by the Chinese government.[22] Soon after Clinton's speech, Harvard Law Professor Jack Goldsmith criticized what he viewed as the Administration's hypocrisy: how could the State Department support the disruption of another state's internet regulations on one hand while praising the rule of law on the other?[23] Though Professor Goldsmith's compelling criticism suggests inconsistency, this problem could be resolved by a continued U.S. commitment to norms in support of universal access to information and electronic free speech. While this is easier said than done, the benefits of more legal principles against restrictions on information and democratic speech could be considerable.[24]

Similar to China, Iran poses challenges to the United States in both the physical and electronic worlds. Following the questionable election results of 2009, reformist youths made every effort to organize and communicate their message through social media. Doing so meant that protesters not only opposed their government in the streets; reformist youths also challenged governmental restrictions on access to such media, including Twitter.[25] Internet and phone connection speeds were purposely slowed to a dysfunctional level, so as to disable Green Movement supporters from uploading photos, video, and other information about what was actually happening on the ground. Such internet restriction, combined with reporters' inability to cover the election aftermath, left ordinary Iranians unable to disseminate the vital understanding of the Iranian situation other then what the regime wanted to communicate. This assertion of internet speech control in Iran stands in stark contrast with U.S. internet freedoms which are not as limited, despite the potential security vulnerabilities. This internet freedom is viewed by many as a critical tool for democratic interests internationally.[26]

Generally, America's increasing reliance on technology provides its enemies with new targets. Because infrastructure targets are extensive and the potential culprits similarly numerous, properly attributing these attacks is difficult and poses a problem for the establishment of a legal bright-line standard. For the law to be applied to a state or other culprit, the law and its definitions must account for material matters of technology. If there is an undeveloped or incorrect understanding of the internet's structure, measures like an internet kill switch and passionate words in support of online freedom of speech may provide little benefit. However, if legislation, policies, and international legal norms are structured on an understanding of the diffuse nature of the internet, it may be possible to address the threats briefly discussed above.

---

22 *See* Clinton *supra* note 15.

23 Jack Goldsmith, *Can We Stop the Global Cyber Arms Race?*, WASH. POST, February 1, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/01/31/AR2010013101834.html.

24 *See* Shackelford, *supra* note 19.

25 Lev Grossman, *Iran Protests: Twitter, the Medium of the Movement*, TIME MAGAZINE, June 17, 2009, *available at* http://www.time.com/time/world/article/0,8599,1905125,00.html.

26 *See* Clinton *supra* note 15 (". . . online organizing has been a critical tool for advancing democracy and enabling citizens to protest suspicious election results . . .").