64 STAN. L. REV. ONLINE 106
March 8, 2012

IN SEARCH OF CYBER PEACE: A RESPONSE TO THE CYBERSECURITY ACT OF 2012

Scott J. Shackelford*

The Cybersecurity Act of 2012, which was recently introduced in the Senate Homeland Security and Governance Affairs Committee, is the latest legislative attempt to enhance the nation's cybersecurity. If enacted, the bill would grant new powers to the Department of Homeland Security (DHS) to oversee U.S. government cybersecurity, set "cybersecurity performance requirements" for firms operating what DHS deems to be "critical infrastructure," and create "exchanges" to promote information sharing. In its current form, the bill is a useful step in the right direction but falls short of what is required. Fundamentally the bill misconstrues the scale and complexity of the evolving cyber threat by defining critical infrastructure too narrowly and relying too much on voluntary incentives and risk mitigation strategies. The Act might improve on the status quo, but it will not foster genuine and lasting cybersecurity. Still, it is preferable to the softer alternative SECURE IT Act proposed by senior Republicans.

Some background on the multifaceted cyber threat is needed to understand the contours of the proposed legislation. Cyber attacks are often broken down into four categories: cyber terrorism, cyber war, cybercrime, and cyber espionage. The most pressing problems are cybercrime and cyber espionage. Although virtually every terrorist group has a web presence, true cyber terrorism remains rare. Similarly, there has not yet been a genuine cyber war. But the Obama Administration has cited estimates that cybercriminals stole as much as

* Scott Shackelford is an Assistant Professor of Business Law and Ethics at Indiana University, Kelley School of Business. He is a graduate of Stanford Law School and earned a Ph.D. in politics and international studies from the University of Cambridge. His forthcoming book on cybersecurity law and policy is entitled *Cyber Peace: Managing Cyber Attacks in International Law, Business, and Relations* (Cambridge University Press, 2012). The author wishes to thank Professor Jamie Prenkert and Amanda Craig for their insightful comments on this piece.

$1 trillion in 2008,[1] a figure greater than the global market in illegal drugs, though the cybercrime estimates are contested.[2] Such figures prompted U.S. Senator Sheldon Whitehouse, a Democrat from Rhode Island, to suggest that "we are suffering what is probably the biggest transfer of wealth through theft and piracy in the history of mankind."[3] Another facet of cybercrime is "hacktivism," such as that carried out by the Anonymous group and others not out for the money but to make a political point. The recent arrests of hackers linked with Anonymous and its progeny demonstrate that governments are taking cybercrime more seriously,[4] but a recent study published by Arbor Networks found that confidence among respondents that law enforcement could stem the tide of hacktivism is at an all time low.[5] Espionage sponsored by nations such as China and Russia is an equally daunting concern. James Lewis of the Center for Strategic and International Studies has called cyber espionage "the biggest intelligence disaster since the loss of the nuclear secrets [in the late 1940s]."[6]

These four categories define policy and legal responses to cyber attacks and parse attacks by motive and means, but they neglect the extent to which both actors and paradigms overlap. The Cybersecurity Act does not treat each of these categories equally. An entire section is devoted to cybercrime, while "espionage" is only referenced once (in relation to training for federal employees), and "terrorism" only appears in the findings section. States, non-state actors, criminal groups, and hactivists regularly launch attacks against systems of all types and levels of sophistication, eschewing easy classification. Thus far, the U.S. government has not done enough to stem the tide, prompting Lewis to note: "We have a faith-based approach [to cybersecurity], in that we pray every night nothing bad will happen."[7]

---

1. *See* CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 2 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. The $1 trillion figure includes intellectual property rights violations as well.

2. *See* Misha Glenny, *Why You Can't Trust the Cybercrime Stats*, WIRED UK (Nov. 6, 2011), http://www.wired.co.uk/magazine/archive/2011/12/ideas-bank/cybercrime-stats.

3. Tim Starks, *Cybersecurity: Learning to Share*, CQ WKLY., Aug. 2, 2010, at 1858, *available at* http://library.cqpress.com/cqweekly/document.php?id=weeklyreport111-000003716158.

4. *See* Carrie Johnson, *U.S. Hunts 'Hacktivists,' Some Ask: Is it Worth It?*, NAT'L PUB. RADIO, Dec. 13, 2010, *available at* http://www.npr.org/2010/12/13/132015315/as-u-s-hunts-hacktivists-some-ask-is-it-worth-it.

5. *But see* Kathleen Hickey, *Can Government Stem the Rise of Hacktivism?*, GCN, Feb. 10, 2012, *available at* http://gcn.com/articles/2012/02/10/ddos-cyberattacks-law-enforcement-survey.aspx (reporting that sometimes the sheer number of hackers involved in cyber attacks stymies prosecutorial efforts).

6. *Cyberwar: War in the Fifth Domain*, ECONOMIST, July 1, 2010, at 26 (alteration in original), *available at* http://www.economist.com/node/16478792.

7. See Ken Dilanian, Privacy Group Sues to Get Records About NSA-Google Relationship, L.A. TIMES (Sept. 14, 2010), http://www.latimes.com/business/la-fi-nsa-google-20100914,0,5669294.story.

Dozens of bills have been proposed over the years to shore up U.S. cybersecurity, including the Lieberman-Collins Bill, which would require DHS to develop a government-wide security strategy, as well as the Rockefeller-Snowe Bill, which relies more on incentivizing the private sector to collaborate with the government on developing standards to secure critical national infrastructure. None have been enacted so far, in part because legislation dealing with cybersecurity faces daunting prospects on Capitol Hill given that the issue involves more than forty committees. To cut through the morass, John McCain, a Republican Senator from Arizona, proposed the creation of a Select Committee on Cybersecurity and Electronic Intelligence Leaks, which would produce comprehensive legislation on the subject.[8] But so far the idea has enjoyed little traction.

There are more similarities than differences between the Act and past cybersecurity reform efforts. Information sharing remains voluntary. Tax breaks for upgrading cybersecurity defenses are glaringly absent, even though the 2011 House Cybersecurity Recommendations encouraged Congress to consider expanding existing tax credits. Audits under the bill would be conducted by the firms themselves and be self-reported. But unlike previous bills such as Lieberman-Collins and Rockefeller-Snowe,[9] the Act would not give the President the power to shut down sections of the private Internet in an emergency—the so-called Internet "kill switch." Much of the media coverage of the bill to date has focused on this absence of a kill switch,[10] ignoring other considerations such as the scope of critical infrastructure and complexity of the problem.

The focus on critical national infrastructure (CNI) in the Act is encouraging given its importance to the U.S. economy and to U.S. national security, and the fact that there is some evidence that these sectors are being targeted increasingly frequently by attackers.[11] But what exactly constitutes critical infrastructure?

Defining CNI in the cyber context is difficult, to say the least. The original President's Commission on Critical Infrastructure Protection identifies five such institutions; the European Commission identifies eleven. When the U.S. Department of Defense unveiled declassified portions of its strategy for cyberspace, former Deputy Secretary of Defense William J. Lynn III announced that

---

8. *See* Ben Pershing, *On Cybersecurity, Congress Can't Agree on Turf*, WASH. POST, July 18, 2011, *available at* http://www.washingtonpost.com/politics/on-cybersecurity-congress-cant-agree-on-turf/2011/07/18/gIQACGCWMI_story.html.

9. The Lieberman-Collins Act was S. 3480, 111th Cong., and the Rockefeller-Snowe was S. 773, 111th Cong.

10. *See, e.g.*, *Senators Renew Push for Cybersecurity Bill, Absent 'Kill Switch'*, FOX NEWS (Feb. 15, 2012), http://www.foxnews.com/politics/2012/02/15/senators-try-again-for-cybersecurity-bill-absent-kill-switch.

11. *See, e.g.*, *New M86 Security Labs Report Reveals Spread of Malware Growing via Social Media, Targeted Attacks and Exploit Kits*, WALL ST. J. MARKETWATCH (Feb. 8, 2012), http://www.marketwatch.com/story/new-m86-security-labs-report-reveals-spread-of-malware-growing-via-social-media-targeted-attacks-and-exploit-kits-2012-02-08.

everything from the electric grid to telecommunications and transportation systems constitute critical national infrastructure, stating that a "cyber attack against more than one [of these networks] could be devastating."[12] The U.K. Center for the Protection of Critical National Infrastructure defines CNI as including communications, emergency services, energy, finance, food, government and public services, health, transport, and water. The benefits of taking an expansive view toward CNI classification are obvious, but drawing the line is difficult.

The Cybersecurity Act designates an industry as "critical" by deciding whether "damage or unauthorized access to that system or asset could reasonably result in the interruption of life-sustaining services . . . ; catastrophic economic damages to the United States . . . ; or severe degradation of national security."[13] But it explicitly omits "commercial information technology product[s], including hardware and software."[14] These omissions hamper the ultimate effectiveness of the bill. There are multiple vulnerabilities even in protected systems, and attackers can enter just as easily through compromised commercial hardware as they can through a virus. Recent U.S. government reports have cited supply chain concerns about hardware and have found components embedded with security flaws.[15]

Another concern is that the Cybersecurity Act relies too much on voluntary disclosure. Relying on firms to "self-certify" and granting them immunity from suit if they are attacked but meet DHS standards is an apt political compromise, but it does not go far enough. Provisions were watered down because IT firms balked at stronger language, and some worry that well-meaning regulations may force companies to focus more on compliance than security. Even if some sectors complain about burdensome compliance standards, however, such regulations do play a vital role in firms' security investment decisions. For the time being, Congress is shying away from more centralized information sharing in favor of incentive-based approaches. Even President Obama has said that his administration would "not dictate security standards to private companies."[16]

---

12. William J. Lynn III, Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy at the National Defense University, Washington, D.C. (July 14, 2011), *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1593.

13. Cybersecurity Act of 2012, S. 2105, 112th Cong. § 103(b)(1)(C) (2012).

14. *Id*. § 103(b)(2)(C).

15. *See* Aliya Sternstein, *Threat of Destructive Coding on Foreign-Manufactured Technology Is Real*, NEXTGOV (July 7, 2011), http://www.nextgov.com/nextgov/ng_20110707_5612.php; *see also Experts Urge Stronger Cyber Regulation Bill*, MSN MONEY (Feb. 16, 2012, 1:11 PM ET), http://money.msn.com/business-news/article.aspx?feed=AP&date=20120216&id=14801708 ("The legislation would limit the number of industries subject to regulation to those in which a cyber attack could cause 'an extraordinary number of fatalities' or a 'severe degradation' of national security.").

16. Ellen Messmer, *Obama: Cybersecurity 'Coordinator' Won't Be 'Czar'*, PCWORLD (May 29, 2009), http://www.pcworld.com/article/165756/obama_cybersecurity_coordinator_wont_be_czar.html.

But there is an argument to be made that cybersecurity failings represent a market failure given the presence of free-riding firms that maximize individual profit but not necessarily the public good,[17] and that Congress should not hesitate to fill this governance gap. Already, though, there are some signs of backpedaling in what initially looked to be likely bipartisan support, and as of this writing hearings continue on the proposed legislation. Senator McCain and a group of seven other Republican senators have released the SECURE IT Act, a competing cybersecurity bill that would give DHS less regulatory power over private businesses managing critical infrastructure but would grant the National Security Agency more authority to manage cyber attacks in real time. Proponents argue that SECURE IT is preferable because it creates less new regulation, relying instead on voluntary information sharing and focusing on federal contractors,[18] but this amounts to even less of a game changer than the Cybersecurity Act. The debate continues, especially given concerns of overregulation, privacy, and civil liberties protections,[19] though some of these concerns are tempered by procedures that the DHS is charged with developing under the Cybersecurity Act.[20]

If we want to change the status quo, accountability and responsibility must be increased throughout the system. Government regulations are a necessary part of that process. But given political realities and the magnitude of the problem, reform must also include relying on the competitive market whenever possible to proactively foster best practices, providing market-based incentives and cyber risk mitigation techniques to firms operating CNI, negotiating new international norms, and educating users to avoid becoming victims of social-engineering attacks like phishing. Cybersecurity cannot truly be enhanced without addressing the myriad governance gaps, which include incomplete regulation of CNI; technical vulnerabilities in the physical, logical, and content layers of the Internet; and legal ambiguities ranging from liability for data breaches to the applicability of international law to cyber attacks. One Act cannot accomplish all that—not even close. But being honest about the magnitude

---

17. *See* ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 41-42 (2007). *But see* Eli Dourado, *Is There a Cybersecurity Market Failure?* (George Mason Univ. Mercatus Ctr., Working Paper No. 12-05, 2012), *available at* http://mercatus.org/publication/there-cybersecurity-market-failure-0 (arguing that market failures are not so common in the cybersecurity realm).

18. *See* Diana Bartz, *SECURE IT Act: Senate Republicans Introduce Softer Cybersecurity Bill*, HUFFINGTON POST, http://www.huffingtonpost.com/2012/03/01/secure-it-act_n_1314213.html (Mar. 1, 2012, 3:17 pm EST).

19. *See* Ellen Nakashima, *NSA Thwarted in Cybersecurity Initiative*, WASH. POST, Feb. 28, 2012, at A1, *available at* http://www.washingtonpost.com/world/national-security/white-house-nsa-weigh-cyber-security-personal-privacy/2012/02/07/gIQA8HmKeR_story.html (reporting on privacy concerns held by the Obama Administration concerning the NSA's attempts to take a more active role in protecting CNI).

20. *See* Paul Rosenzweig, *Information Sharing and the Cybersecurity Act of 2012*, LAWFARE (Feb. 14, 2012, 6:43 PM), http://www.lawfareblog.com/2012/02/information-sharing-and-the-cybersecurity-act-of-2012.

of the problems we face would help to begin a national conversation about what needs to happen next.

In *3001: The Final Odyssey*, Arthur C. Clarke envisions a future in which humanity had the foresight to rid the world of its worst weapons of mass destruction by placing them in a vault on the moon. A special place in this vault was reserved for the malignant computer viruses that, in Clarke's speculative fiction, had caused untold damage to humanity over the centuries. Before new cyber attacks do untold damage to our information society, it is in our interest to educate and regulate our way to a steady state of cybersecurity. Part of this process involves broadening the definition of CNI in the Cybersecurity Act and deepening public-private partnerships through more robust information sharing. Science fiction teaches us that our future world can be either a wonderful or a dystopian place. Whether or not the future includes the security and prosperity of cyber peace is up to us—including, for better or worse, the U.S. Congress.

A COVID-like global cyber pandemic is inevitable. Here are 3 lessons from the coronavirus crisis on how the world can better prepare for it and respond.Â How the Forumâ€™s networks have navigated the global response to COVID-19. Read more about this project. Explore context.Â The only way to stop the exponential propagation of cyber-COVID would be to fully disconnect all vulnerable devices from one another and the internet to avoid infection. The whole world could experience cyber lockdown until a digital vaccine was developed. All business communication and data transfers would be blocked. â€˜cyber peaceâ€™ is then deî€žned and the components that make such a state possible. identiî€žed. The last section discusses the different roles and their responsibilities to. reach and preserve a state of peace in the digital sphere, coming to the conclusion. that the Internet is not in a state of cyber war but more in a state of negative or. unstable peace. To protect the Internet as a critical infrastructure from being abused.Â Computer Emergency Response Team (GovCERT) of the Swiss Government, Bern University. of Applied Science, Bern, Switzerland. e-mail: reto.inversini@lab42.ch. Cyber Peace Foundation (CPF) is an award-winning civil society organization, think tank of cyber security and policy experts with the vision of pioneering Cyber Peace Initiatives to build collective resiliency against cyber crimes & global threats of cyber warfare.Â Global Cyber Challenge- 2017. Global Cyber Challenge was an important part of Global Conference on Cyber Space (GCCS), 2017 being inaugurated by the Honâ€™ble Prime Minister of India and being attended by nearly 120 countries. Round Tables. Cyber Peace Foundation. Donate. Help Us Make a Difference Today. Join the Cyber Peace Corps. Be a part of the global volunteer network. eSaksham. Welcome to cyberpeace foundation. Is cyber peace possible? There is an urgent need for global rules around state conduct in cyberspace. But, building new norms is a slow and complicated process â€” is the UN up for the task?Â These proposed restraint measures seek to provide a protective status to critical infrastructure and to the cyber emergency response teams that are crucial to mitigating the effects of a damaging cyber attack. In this respect they mirror the protective status afforded civilian facilities and â€˜first respondersâ€™ under international humanitarian law, although importantly the GGE proposal would appear to extend this protection to peacetime conditions and not limit it to situations of armed conflict. What is cyber peace and security? The word â€œcyberâ€ has come to refer to an ever-widening spectrum of activities encompassing espionage, surveillance, privacy intrusions, denial-of-service attacks, ransomware, and malware operations that variously impact nations and individuals. Many of these activities have the ability to disrupt, disable, or destroy vital physical infrastructure or national or human security and well-being.