The Journal of Science Policy & Governance

POLICY MEMORANDUM:

INCREASE CYBER-SECURITY VIA INTERNET GOVERNANCE, REPORTING, AND AWARENESS REFORMS

BY

FARID E. BEN AMOR

University of Southern California

fbenamor@gmail.com

To: Assistant Secretary Greg Schaffer, Department of Homeland Security
From: Farid E. Ben Amor
Date: January 1, 2012
Subj.: Increase cyber-security via Internet governance, reporting, and awareness reforms

Executive Summary

The inchoate Internet is increasingly essential to daily life and the health of the economy yet it stands stunningly unsecured. The packet-switching nature of the Internet, while responsible for its fundamentally free flow of information, renders critical public infrastructure, banks, and private industry vulnerable to attack that can lead to theft of personal or corporate information and immobilization. To achieve the goal of escalating Internet security in our homeland, analysis suggests better agency oversight through governance integration and targeted measures to augment personal and corporate awareness and accountability.

Issue

Vulnerability of U.S. Internet Infrastructure

To understand the potential damage to the U.S., it is germane to look at the Internet disruptions that occurred in Estonia in 2007—one of the world's first cyber-wars. In April 2007, Estonia moved a Soviet memorial statue and the country's Internet network promptly came under attack from sources within Russia. Through a sustained distributed denial-of-service (DDoS) attack, non-state actors brought Estonia's Internet-dependent activities to a grinding halt, and for weeks its 1.3 million residents had difficulty accessing banks, communications, even electricity in some areas (Lesk, 2007).

Though the U.S. is much larger than Estonia, over 90% of online traffic in the country travels through the cables of just five companies: Verizon, Qwest, Level 3, Sprint, and AT&T (Clarke and Knake, 2010). This centralized administration holds many risks, like reducing the robustness of redundancy. The lack thereof may allow a well-placed logic bomb via a worm or other malicious program to wreak havoc, resulting in billions of dollars of harm across private and public sectors (U.S. Department of Homeland Security [DHS], 2011b). These vulnerabilities cost relatively little to exploit and can cause grave economic damage.

With so much of the country reliant on the Internet, a team at Carnegie-Mellon University attempted to track how many such attacks occur per year and in 2003 recorded over 137,000 incidents (Kruger et al., 2007). That was the last year they counted cyber-attacks as the task simply became too onerous (Ibid). Significant damage in the U.S. has only been avoided so far because the largest worms have been developed and distributed without payloads. As a result, the most effective and potentially destructive viruses have come as a result of creative experimentation and, through reverse-engineering, ultimately benefitted the network security community (Zittrain, 2006). Nonetheless, the opportunity cost and time spent to fix issues has harmed every American at some point, whether through personal use or indirect corporate or infrastructure injury.

Technical design vulnerabilities

The Internet was created by piecemeal as a network that facilitates information sharing. Security was not an initial concern so many vulnerabilities exist (Cerf, 2009). From its origins as an academic experiment in the 1960s funded by the Defense Advanced Research Projects Agency

(DARPA), the Internet's essentially free, unrestricted packet-switching is dependent upon the goodwill of the whole (Cerf, 2009). Cerf argues that the most significant imperative to its architecture is indeed its interoperability, and it holds true for all actors, from industry to governments. These characteristics also compose the Internet's critical vulnerability: naiveté. In other words, any link in the chain accepts all incoming packets and passes them forward, assuming good faith as with Estonia's DDoS attacks.

Similarly, in 1995 a team led by Jon Postel subverted the domain name system (DNS) in an attempt to shift management from Network Solutions—a private company with singular authority over domain names—to a nonprofit organization. The DNS translates web address names such as www.whitehouse.gov to a matching numerical Internet address. Postel's team caused such web addresses to point to his computer rather than the proper content located on the root server managed by Network Solutions (Benkler, 2006). Such susceptibility is endogenous to the Internet's technical nature.

Unmonitored malicious actors

Whether it's a state declaring war, a rogue terrorist group, or even a bored teenager, just about anyone can pirate online corporate or public systems. Many options are available to hackers engaging in industrial espionage to steal American innovations, content, and money, or shut down electric grids, etc. The anonymity endemic to the Internet makes the cyber-threat to our way of life unpredictable and thus less preventable. Moves to seek the power of attribution through technical circumvention are noted as detrimental to Internet innovations (Internet Security Alliance, 2008). Such efforts in the past have also found strong resistance from privacy advocates (Madsen, 1998). Similarly, blind (non-targeted) filtering has significant opposition from technical infrastructure companies. Without such embedded technology to readily unveil perpetrators, the Internet is simply too large to monitor effectively.

Governance fragmentation

The political context surrounding Internet regulation has long delayed significant action in reducing threats. The United Nations empowered Internet Governance Forum (IGF) continues to press for equal consideration of privacy, openness, and security, but their lack of collaboration with government leaders undermines real authority (Gutterman, 2011). The U.S. administration has also shifted priorities, with the Bush White House seeking brute circumvention tools such as embedded "backdoors" similar to the Clipper chip to preserve critical infrastructure (White House, 2003). The current administration's policy instead seeks to protect the Internet while still maintaining online openness and emphasizing the retention of intellectual property (White House, 2010). With the ever-mounting economic reliance on the Internet, the window for agencies to act is imminent. Reuters also reports that bipartisan support could exist to advance the President's cyber-security agenda through DHS (MacInnis, 2011). Nonetheless, Internet authorities continue to be dispersed across multiple agencies, especially on the international stage. However, the department's proposed 2012 budget aims to realign its coalition-building capacity in its National Cyber-security and Communications Integration Center (NCCIC; U.S. DHS, 2011a).

Policy Options

Alternative I: Kill switch

The ability for the President to restrict or disable Internet access across the country is commonly known as the kill switch alternative. Its objective is to shield information systems in the U.S. from further damage in a cyber-attack. This circumvention tool was most notably used in Egypt during the civil unrest, and on a more limited but continuous basis in Russia and China (Roberts, Zuckerman & Palfrey, 2011). Some proponents argue that the uniqueness of cyberspace as opposed to any other battlefield lends itself to an effective preemptive shutdown (Ackerman, 2011). If the U.S. is attacked in the physical world, the attacker and the motive for the attack predicate the legal and military response. In the virtual world, these are precisely the two unknown elements (Ibid). Launching such a defensive response would then head off further damage and neuter the attack. The mechanism is a technical one embedded as a blind (non-targeted) filter within the Internet's infrastructure and Internet Service Providers (ISPs), altering and delaying the way packets are managed.

Alternative II: Governance integration

This alternative consolidates Internet security regulation through the expansion of the NCCIC's authorities to become the National Center for Cyber-security and Communications (NCCC) with a goal of resolving the severe fragmentation of security responsibility. Authorities to regulate Internet security are greatly dispersed across many agencies and even international bodies. To demonstrate, the Securities and Exchange Commission (SEC) is able to set reporting requirements in the financial services industry, while the IGF and Internet Corporation for Assigned Names and Numbers run web resolution security. Currently, Internet security task forces within the Commerce Department and elsewhere also operate independently (U.S. Government Accountability Office, 2005). There are over 30 competing bills pending before the Congress to attempt to ameliorate Internet governance and security issues. Integration serves to streamline all activities involving Internet security operations through one place and enhance targeted filtering in the NCCC. The method requires Congressional approval and would complement the Secretary's current lobbying agenda in the Congress.

Alternative III: Awareness and accountability

Incorporating several externally-oriented actions, the final alternative focuses on information dissemination through education and mandatory reporting of critical data breaches, thus increasing the public's sense of responsibility for its online security. Mandatory reporting of data breaches in critical sectors, particularly banks, Internet infrastructure, utilities, and other industries would encourage these parties to accept its role in defending its systems or face backlash from consumers (Internet Policy Task Force, 2011). To help accommodate the increased financial burden with these investments, DHS would also serve as a clearinghouse for cyber-insurance so that capital costs are significantly lowered. The department would also build on its rich tradition of educating the public about security hazards. The recently inaugurated National Cyber-security Awareness Campaign ("Stop, Think, Connect") would be expanded to promote citizen awareness in online environments (U.S. DHS, 2011b). It would also set national standards of security so that both individuals and companies would have a measure with which to gauge its online protection status.

Evaluation of Options

All alternatives require at least some level of Congressional approval and public support. The recent flurry of Internet policy activity with the discussion of the Stop Online Piracy Act (SOPA) and the PROTECT IP Act highlight the excitement and controversial nature of non-targeted filtering. Stakeholders are highly invested in securing this vital public resource while taking care to note potential unnecessary violations of choice and web freedom. Public satisfaction (and information) cannot be outweighed by the profundity of the solution and the alternatives presented are evaluated on these merits.

Alternative I: Kill switch

Although the kill switch alternative was part of a leading Internet security package in the US Senate, it is a pareto inferior alternative for both government and the public. Castrating a large portion of the US economy in one fell swoop will likely cause far more economic and political damage than any external attack due to its absolute inclusion, which is also the marker of its effectiveness. Despite the concept's continued support from some prominent cyber-security professionals, the political fallout from the kill switch's presence in a recent bill caused its politically moderate sponsors (Senators Lieberman and Collins) to issue a hurried press release aimed at dispelling fears that any such language would reappear in their comprehensive cyber-security bill (Ackerman, 2011). The recent opposition to SOPA on the exaggerated accusations of censorship in its proposed DNS filtering emphasizes the unpopularity of a shut down. Given the scant support for this technical boondoggle – and its potential harm – DHS should not pursue this alternative.

Alternative II: Governance integration

Efficiency and targeted filtering are the primary objectives of the proposed consolidation of cyber-security responsibilities within the DHS. There is some capital outlay associated with this direction, but it is difficult to place a dollar value on the quality of life preserved and secured through the continued functionality of the Internet and the protection of intellectual property (Kelman, 1981). Political costs are also at risk as many senators and congressmen prefer different federal fixes. But, the current furor over SOPA ought to guide our attention towards better public information about the necessary security and efficiency measures in the proposals while working with lawmakers to eliminate excessively broad language and enhance feasibility. The administration has announced its support for the defense of intellectual property and integration to occur within the DHS as proposed in this alternative (White House, 2010). The department continues to enjoy support from the relevant committee chairmen, including Senator Lieberman and his bipartisan colleagues. Also, DHS has the interim ability to hire approximately 1,000 more staff for cyber-security and has successfully served as the command center for many other data security operations (Ibid). Finally, the history of this department's establishment as a centralization and command clearinghouse lends itself well to adopt oversight of this security issue.

Alternative III: Awareness and accountability

If cyber warfare were to break out, most of the assets damaged would be commercially owned, jeopardizing thousands of jobs (Etzioni, 2011). This affects populations well beyond corporate shareholders and thus demands a regulatory solution to address this market failure. Unsurprisingly, the financial industry and infrastructure lobby are fighting these additional costs and potential requirements. Regardless, the benefits of passing these increased securities enormously outweigh the alternative of clamping down on the Internet to protect it through an intervention tool like the kill switch. Furthermore, the accountability and transparency elements have found political support among moderate Republicans, while Democrats overwhelmingly embrace Internet security education for digital literacy. The grassroots nature of this alternative rather than any excessive controls – once beyond the initial backlash – will also ultimately lead to more appropriate and prudent security measures relative to the company's business. It is also important to note that at this point, not even elementary requirements have been introduced and even requiring that preinstalled security software is turned on in software packages would drastically increase security across the board. The department should vigorously pursue this set of policies.

Recommendation to advance alternatives II and III

DHS must better prepare for cyber incidents by embracing the latter alternatives of governance integration, smart filtering, awareness, and accountability. Together they optimally work towards the goals defined by the problem and fall within the purview of what is feasible for the department to request and accomplish. These alternatives – in tandem – address what the Secretary sought before the Congress in October: the right balance between government action and private responsibility – also likely to appeal to both sides of the aisle (Associated Press, 2011). Despite posing a significant cost and non-adherence to PAYGO (budget-neutrality), security bills traditionally receive wide political support. These alternatives also use elements from nearly all of the 32 pending bills, which enhance its political likelihood of passing. With the support of the Congress potentially in alignment with the President on the defense of intellectual property and the Internet as we know it, the timeline could be greatly curtailed with the country's Internet infrastructure on a vastly more secure footing.

Conclusion

The cyber-security threat to the US is real and serious, potentially undermining our economy and way of life. Protecting this digital homeland necessitates immediate action while taking care to avoid damaging its intrinsically open nature and status as a commons. Our objectives are optimally achieved leaving the blunt non-specific tools out of it and educating the public first – thus avoiding the sudden burst of outcry over bills like SOPA – and instead consolidating resolution authority in the NCCIC/NCCC. Through it, the department should pursue mandatory transparency of data breaches, while offering incentives and education to expand corporate and public defenses and awareness of online dangers. The Department of Homeland Security is best situated to build the coalition to concurrently address these Internet security issues.

References

Ackerman, L. (2011). Internet “kill switch” legislation: Can Obama turn off the Internet? *Berkeley Technology Law Journal*, *BOLT*, 3/9/11. Retrieved from http://btlj.org/2011/03/09/internet-kill-switch-legislation-can-obama-turn-off-the-internet/

Associated Press. (2011, October 20). FBI official says secure, alternate Internet is needed to protect critical systems. *The Washington Post*. Retrieved from http://www.washingtonpost.com/national/pentagon-finalizing-policies-on-appropriate-response-by-military-to-cyberattacks-against-us/2011/10/20/gIQAIDtb0L_story.html

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale University Press.

Cerf, V. (2009). The day the Internet age began. *Nature, 461*, 1202-1203.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins Publishers.

Etzioni, A. (2011). Cyber-security in the private sector. *Issues in Science and Technology, Fall 2011*, 58-62.

Gutterman, B. (Ed.). (2011). *Developing the future together: The fifth meeting of the Internet Governance Forum*. Vilnius, Lithuania: United Nations. Retrieved from http://www.intgovforum.org/cms/2011/book/IGF_2010_Book.pdf

Internet Policy Task Force. (2011). *Cybersecurity, innovation, and the Internet economy*. Washington: U.S. Department of Commerce. Retrieved from http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf

Internet Security Alliance. (2008). *The cyber security social contract: Policy recommendations for the Obama administration and 111th Congress*. Arlington: Internet Security Alliance. Retrieved from http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf

Kelman, S. (1981). Cost-benefit analysis: An ethical critique. *AEI Journal on Government and Society Regulation*, 33-40.

Kruger, L. G., Moteff, J. D., Gilroy, A. A., Seifert, J. W., Figliola, P. M., & Tehan, R. (2007). *Internet: An overview of key technology policy issues affecting its use and growth* (Order Code 98-67). Washington: Congressional Research Service.

Lesk, M. (2007). The new front line: Estonia under cyberassault. *IEEE Security & Privacy, 1540-7993,* 76-79.

MacInnis, L. (2011, October 20). Obama officials, Senators agree to seek cyber deal. *Reuters*. Retrieved from http://www.reuters.com/article/2011/10/21/us-usa-cyber-senate-idUSTRE79K03H20111021

Madsen, W. (1998). *Critical infrastructure protection and the endangerment of civil liberties: An assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)*. Washington: Electronic Privacy Information Center. Retrieved from http://epic.org/reports/epic-cip.html

Roberts, H., Zuckerman, E., & Palfrey, J. (2011). *2011 Circumvention Tool Evaluation*. Cambridge: Berkman Center for Internet & Society. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2011_Circumvention_Tool_Evaluation_1.pdf

U.S. Department of Homeland Security. (2011a). *Budget in brief: Fiscal year 2012*. Washington: U.S. Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf

U.S. Department of Homeland Security. (2011b). *Enabling distributed security in cyberspace: Building a healthy and resilient cyber ecosystem with automated collective action*. Washington: U.S. Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

U.S. Government Accountability Office. (2005). *Department of Homeland Security: A comprehensive and sustained approach needed to achieve management integration* (GAO-05-139). Washington: U.S. Government Accountability Office.

White House. (2003). *The national strategy to secure cyberspace*. Washington: White House. Retrieved from http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

White House. (2010). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. Washington: White House. Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Zittrain, J. (2006). *The Generative Internet* (University of Oxford Faculty of Law Working Paper 28). Cambridge: Berkman Center for Internet & Society.

About the Author

Farid E. Ben Amor works in media rights at Warner Bros and just prior helped acquire programming at DIRECTV and pursuing his graduate studies at USC in public policy affairs. Before that, Farid spent time in Washington DC, most recently as Deputy Field Director of the financial reform campaign to fix Wall Street and create a Consumer Financial Protection Bureau. In addition he also worked on various electoral, media policy, and direct action campaigns, ranging from Obama for America to an effort to digitally empower low-income communities at ACORN. Prior to these, Farid worked in U.S. Senate committee and member offices as a Legislative Aide and attended Cornell University where he studied Physics.