SCUSA 64
Leading in Lean Times:
Assuring Accountability and Assessing American Priorities in an Age of Austerity

American Security in a Networked World: Emerging Challenges in Cyberspace

Cyberspace is a complex, fragile, and ever-changing ecosystem. America is growing more dependent on it with each passing day, connecting more than two billion people around the globe to conduct business, share information and ideas, and socialize.[1] At the same time, cyber threats continue to increase in sophistication and volume, putting all in the global networked commons at risk.

Increased cybersecurity is vital to protecting America's national security interests, critical infrastructure, and intellectual property. Adversaries ranging from foreign state actors to corporate spies continue to exploit vulnerabilities in U.S. networks, systems, and practices.[2] With millions of dollars worth of intellectual property, vital national resources such as power grids and banking systems, and design plans for the latest military defense equipment at risk every day, it is critical for U.S. policymakers to understand the problems involved and find solutions. A fundamental cyberspace policy goal should be to enable the country to continue to enjoy the tremendous social, economic, and other gains that cyberspace has made possible, while minimizing the associated risk.

While lean times may do little to slow the growth of cyberspace, they pose challenges for safeguarding it. Despite growth in cybersecurity budgets across the federal government, threats and vulnerabilities are increasing at an alarming rate that is likely to outpace efforts to protect cyberspace for commerce, government, and individual enjoyment. Current cyber expenditures focus on government – primarily military – capabilities and do little to address cybersecurity in the commercial and public domains. This paper explores the landscape of cyberspace, emerging challenges in cyberspace, and potential opportunities to focus American policy during lean times.

The Landscape of Cyberspace

Cyberspace is defined in National Security Presidential Directive 54 (NSPD-54) as the "interdependent network of information technology infrastructures, [including] the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[3] Over the past twenty years, businesses, governments, and individual citizens have gradually discarded many of the manual systems and processes in their daily lives and replaced them with more efficient automated – and increasingly networked – systems spread across cyberspace. Unfortunately, the underlying infrastructure of cyberspace and the

[1] Matthieu Pelissie du Rausas et al., "*Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity*," (McKinsey Global Institute, 2011), accessed 10 September 2012, http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/internet_matters.
[2] Jon Brickey, Jacob Cox, John Nelson, and Gregory Conti, "The Case for Cyber," *Small Wars Journal*, September (2012), http://smallwarsjournal.com/jrnl/art/the-case-for-cyber.
[3] National Security Presidential Directive 54

applications that rely on it have not historically been designed with security as a primary concern and are constantly changing. Demands on the telecommunications backbone infrastructure outstrip capability and capacity, pushing the boundaries of technology and policy.

At the same time, cyberspace is the newest domain for spies, criminals, terrorists, activists, and even militaries to do what they have done in the analog world, but now more efficiently and anonymously. Norms, laws, and treaties lag the innovations of these actors, creating lawlessness reminiscent of a modern day Wild West: a space full of opportunities for freedom and prosperity and, at the same time, danger.

A Realm for Peace

One prevalent view of cyberspace holds that it should be a global networked commons, allowing peaceful freedom *of* the Internet and *via* the Internet.[4] According to this view, these freedoms apply to all activities in cyberspace to include commerce, communications, and other forms of interaction. Current U.S. cyberspace policy asserts the government's role to safeguard America's democratic traditions and ensure the privacy rights and civil liberties guaranteed in the Constitution. Comments by Secretary of State Clinton indicate U.S. foreign policy extends the concept of freedom of the Internet to not only U.S. citizens, but citizens of all nations. Recently Clinton chastised the Chinese government's restriction of Internet access, saying the United States "would push to preserve the ability of anyone to connect and freely transfer information over the Web."[5] What means should the United States employ to back such comments? Would they risk promoting cyberspace as a warfighting domain to preserve the possibility of peace?

Cyberspace as a Warfighting Domain

Nation states such as China, Russia, Iran, Israel, and the United States train units of cyber warriors to operate in cyberspace, though critics believe that cyberwar is hype and will never happen.[6] Whether a cyber-only war will happen is debatable; however, many military analysts believe the Russians used a cyber attack to augment its conventional attack on Georgia in the 2008 South Ossetia War.[7] Post-war analysis alleges that Russian cyber forces – consisting of skilled hackers from nationalist groups, the Russian Business Network criminal gang, and the military – attacked Georgian media sites, government sites, and Internet service providers using persistent distributed denial-of-service attacks.

America's stance on the militarization of cyberspace became clearer in July 2011 when it added cyberspace as a warfighting domain and developed a military strategy for cyberspace.[8] As part of the strategy, the United States established military cyber units to prevent adversaries from exploiting, disrupting, denying, or degrading Department of Defense networks and systems.

---

[4] Richard Fontaine and Will Rogers, "*Internet Freedom: A Foreign Policy Imperative in the Digital Age*," (Center for a New American Security, 2011), accessed 12 September 2012, http://www.cnas.org/files/documents/publications/CNAS_InternetFreedom_FontaineRogers_0.pdf.

[5] Cecilia Kang, "Hillary Clinton Calls for Web Freedom, Demands China Investigate Google Attack," *The Washington Post*, 22 January 2010.

[6] Audrey Guinchard, Between Hype and Understatement: Reassuring Cyber Risks as a Security Strategy, *Journal of Strategic Security*, 4:2 (2011): pp. 75-96.

[7] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January (2011), http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[8] Department of Defense, Department of Defense Strategy for Operating in Cyberspace, (Department of Defense: Washington, 2011), 1-6.

Though most of the published strategies discuss defensive measures, the United States expressly reserves the right to conduct offensive cyberspace operations, which it reportedly did in the 2010 Stuxnet attacks on Iranian nuclear enrichment facilities.[9] If America was behind the Stuxnet attack, what does that say about U.S. cyberspace doctrine? Was Stuxent a preemptive strike signaling a new Cold War – or, more precisely, a Code War?

Emerging Challenges

While experts may disagree on the severity of malicious cyber activities and their potential consequences, few dispute the pervasive nature of current vulnerabilities in organizations, networks, and processes. These vulnerabilities stem from a combination of human, technical, and policy causes, and they pose significant security challenges for cyberspace.

Standards

One challenge relates to the development, promulgation, and enforcement of enhanced cybersecurity standards. Different stakeholders hold varying views about the merits of additional cybersecurity standards or regulations. One perspective holds that a government agency should promulgate a gold standard, developed in collaboration with industry, and should have the authority to enforce this standard. Another perspective, which generally receives greater support from within the private sector, claims that industry should develop its own cybersecurity standards, in coordination with government agencies, which would ideally also draw on the best available thought in academia. Advocates of this view usually argue that standards, incentives, and government-industry collaboration should all be part of the solution, which must also take cost effectiveness into account and be able to move rapidly – likely more rapidly than a coordinated government-approved solution. As an additional complicating factor, the issue of standards becomes a very complex challenge for global enterprises that need to operate in accordance with the standards and regulatory regimes of multiple government jurisdictions.

Defensible Networks and Systems

Another important challenge relates to the need to build and maintain more defensible networks and systems. Cybersecurity experts in the public and private sectors, and increasingly non-technical organizational leaders at the executive level, realize that cyber security threats are evolving and escalating rapidly. Security vulnerabilities are most troubling in the case of companies that operate critical infrastructure such as the electric grid, dams, and the servers that process financial transactions. These companies are clear targets since their operations affect public safety. While most companies accept at least a degree of responsibility for the protection of their own networks, it not clear that they are capable of providing themselves with robust security.[10] This may be due, in part, to a gap in cybersecurity awareness, knowledge, and capabilities, but this situation also stems from the fact that existing economic incentives are not sufficient – in many cases – to generate adequate cybersecurity. This is a classic example of market failure and an opportunity for government to assist. An additional factor is that the most

[9] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012.
[10] Gavin O'Gorman and Geoff McDonald, "The Elderwood Project," (Symantec, 2012), accessed 11 September 2012, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

capable actors in cyberspace are states and, as a general rule, individual companies expect assistance from the government in protecting themselves from malicious actors supported by state resources.

Coordination and Authorities

A third challenge is the need for effective coordination among U.S. government entities with various roles and responsibilities relating to the protection of U.S. interests and values in cyberspace. Currently, responsibility for the various domains of the Internet is distributed across multiple agencies. For example, the Department of Defense has the lead for military and national security networks, the Federal Bureau of Investigation (FBI) has the lead for law enforcement and counterintelligence, and the Department of Homeland Security has the lead for the rest of the government's networks and for orchestrating coordination with private sector critical infrastructure providers. Since there is no single government department or agency in charge, efforts to protect the country require extensive coordination and collaboration. Faced with malicious actors who lack such organizational constraints, or who may seek to exploit them, it is imperative that there be extensive coordination and collaboration among U.S. government departments and agencies to enable an integrated response.

Coordination implies information sharing across organizational lines, which can be challenging, whether these lines are between private sector entities, government departments and agencies, or across the public-private divide. These challenges stem primarily from policy limitations, competing business interests, fears of financial liability, and concerns surrounding civil liberties.

Opportunities

Securing cyberspace as a global commons for all purposes will require resources from individuals, businesses, and especially government. There are, however, opportunities in these lean times to strategically focus resources to achieve national objectives.

Reorganization

Since the number and severity of cyberattacks continue to rise, is America capable of turning the tide of cyber with current organizations and authorities? The lead organization – the Department of Homeland Security – is fairly new and is responsible for a very broad portfolio of security challenges. While it is appropriate for Department of Homeland Security to have the lead, the Department of Defense has a significant role to play in providing support, mainly because it has been the recipient of the majority of the government's investment in cybersecurity capabilities to date. The FBI, which must bring its law enforcement and counterintelligence authorities to bear, is an additional essential partner. Is the status quo sufficient for protecting cyberspace? Have American policymakers deferred national security to the market? Has the cybersecurity market failed? Is it time to consider a new national cyber agency?

A Manhattan Project for *Cyberspace*

The infrastructure of cyberspace was not designed for current or future demands. The Internet was originally designed for open, though not secure, communication. As a result, it is far too easy to wreak havoc while hiding behind spoofed identities and locations. These basic architectural problems may be some of the hardest to address because it may be easier to build a

new and improved Internet than retrofit the existing one. Such a project would need to be on par with the Manhattan Project in terms of the resources, vision, and determination required. A cyber project of this scale could easily cost several hundred billion dollars, which, during a time of austerity, complicates this as an option. Should the United States (in coordination with international partners) build a new Internet with advanced security measures to ensure confidentiality, integrity, and availability? Who would govern this new Internet? Most importantly, what policies for a new Internet would safeguard America's democratic traditions and ensure Constitutional rights and liberties?

Barriers to Action

Any significant policy effort requires a team approach and at least a majority agreement between the legislative and executive branches of government. Members of Congress understand the need for legislation to address cybersecurity challenges, though they disagree on the specifics. Congress has been working on draft legislation addressing several cybersecurity challenges; unfortunately, there is no consensus yet on two key pieces of legislation: the Secure IT Act and the Cybersecurity Act of 2012. As the prospects for legislative consensus dwindle in an election year, the President is considering his authority to issue executive orders to address some of the critical cybersecurity challenges.[11]

Though government regulation could have a positive impact on ensuring civil liberties and providing security, it cannot solve all problems. Regulation usually comes with a price tag, and there is only so much one can ask of the private sector in lean times. At the same time, the federal government will have a hard time selling large projects or new organizations to taxpayers. All of these policy opportunities must be part of a larger cyberspace strategy that brings together all the elements of national power and partnerships with the private sector and academia.

Conclusion

Lean times present challenges to U.S. policymakers trying to keep pace with the burgeoning threats in cyberspace. The American public expects its government to defend the country from external threats, including those in cyberspace, protect public safety, and promote prosperity. Since the domain is relatively new and the public's knowledge is nascent, debates concerning policies, laws, and strategies are just taking shape in the field and across the broader society. As these debates take place and governance frameworks evolve, commercial and intellectual freedoms in cyberspace should and must remain central considerations. Lean times also present opportunities to focus efforts and shape new policies reflecting American ideals, concerns, and priorities. Although democratic deliberation is vital and can be expected to take time, the security risks and challenges are already here. The militarization of cyberspace has begun—the genie is out of the bottle.

[11] Brendan Sasso, "After Defeat of Senate Cybersecurity Bill, Obama Weighs Executive-Order Option," *The Hill*, 4 August 2012.

Recommended Readings

Lewis, James A. "Why Privacy and Cyber Security Clash." In *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II, edited by Kristin M. Lord and Travis Sharp, 123-142. Center for a New American Security: Washington, 2011.

http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. RAND Corporation: Santa Monica, 2009.

http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Obama, Barack H. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. The White House: Washington, 2011.

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Jon Brickey, Jacob Cox, John Nelson, and Gregory Conti, "The Case for Cyber," *Small Wars Journal* 8:9 (13 September 2012).

http://smallwarsjournal.com/jrnl/art/the-case-for-cyber

Cecilia Kang, "Hilary Clinton Calls for Web Freedom, Demands China Investigate Google Attack," *The Washington Post* (22 January 2010).

http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699_pf.html

Matthieu Pelissie du Rausas, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui, and Remi Said, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity*, (McKinsey Global Institute, 2011).

David Hollis (2011), "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, (6 January).

http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Brendan Sasso (2012), "After Defeat of Senate Cybersecurity Bill, Obama Weighs Executive-Order Option," *The Hill* (4 August).

http://thehill.com/blogs/hillicon-valley/technology/242227-with-defeat-of-cybersecurity-bill-obama-weighs-executive-order-option.

Additional Readings

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Department of Defense: Washington, 2011.

http://www.defense.gov/news/d20110714cyber.pdf.

Fontaine, Richard and Will Rogers. *Internet Freedom: A Foreign Policy Imperative in the Digital Age*. Center for a New American Security: Washington, 2011.

http://www.cnas.org/files/documents/publications/CNAS_InternetFreedom_FontaineRogers_0.pdf.

Nye, Joseph S. Jr. "Power and National Security in Cyberspace." In *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II, edited by Kristin M. Lord and Travis Sharp, 5-24. Center for a New American Security: Washington, 2011.

http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf.

Segal, Adam. "Cyberspace Governance: The Next Step." In *Policy Innovation Memorandum No. 2*. Council on Foreign Relations: New York, 2011.

http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

Singer, Peter W. and Noah Shactman. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive." Brookings Institution: Washington, 2011.

http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx.