Week 05 – Writing Assignment 02

William Slater

DET 630 – Cyberwarfare and Cyberdeterrence

Bellevue University

U.S. Policy Appraisal Related to Cyberwarfare and Cyberdeterrence

Matthew Crosston, Ph.D. - Professor

September 30, 2012

U.S. Policy Appraisal Related to Cyberwarfare and Cyberdeterrence

This brief paper will discuss U.S. Policy related to cyberwarfare and cyberdeterrence.

Current U.S. Policy Covering Cyberwarfare Threats

The current written policy related to cyberwarfare threats can be found in President Obama's Defense Strategic Guidance 2012, a 16-page policy documented that was published on January 3, 2012. The excerpt related specifically to cyberwarfare and cyber threats is shown below:

> "To enable economic growth and commerce, America, working in conjunction with allies and partners around the world, will seek to protect freedom of access throughout the global commons — those areas beyond national jurisdiction that constitute the vital connective tissue of the international system. Global security and prosperity are increasingly dependent on the free flow of goods shipped by air or sea. State and non-state actors pose potential threats to access in the global commons, whether through opposition to existing norms or other anti-access approaches. Both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland. Growth in the number of space-faring nations is also leading to an increasingly congested and contested space environment, threatening safety and security. The United States will continue to lead global efforts with capable allies and partners to assure access to and use of the global commons, both by strengthening international norms of responsible behavior and by maintaining relevant and interoperable military capabilities (Obama, 2012)."

The first explicit Obama Administration policy acknowledging the realities of cyber threats were published in a 30-page document titled International Strategy for Cyberspace in May 2011.

> "Today, as nations and peoples harness the networks that are all around us, we have a choice. We can either work together to realize their potential for greater prosperity and security, or we can succumb to narrow interests and undue fears that limit progress. Cybersecurity is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives. While offline challenges of crime and aggression have made their way to the digital world, we will confront them consistent with the principles we hold dear: free speech and association, privacy, and the free flow of information.

> "The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just, and peaceful conduct among states and peoples have begun to take hold. It is one of the finest examples of a community self-organizing, as civil society, academia, the private sector, and governments work together democratically to ensure its effective management. Most important of all, this space continues to grow, develop, and promote prosperity, security, and openness as it has since its invention. This is what sets the Internet apart in the international environment, and why it is so important to protect.
>
> "In this spirit, I offer the United States' International Strategy for Cyberspace. This is not the first time my Administration has address the policy challenges surrounding these technologies, but it is the first time that our Nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues. And so this strategy outlines not only a vision for the future of cyberspace, but an agenda for realizing it. It provides the context for our partners at home and abroad to understand our priorities, and how we can come together to preserve the character of cyberspace and reduce the threats we face (Obama, 2011)."

How long has this policy been in place? Have any changes occurred to the policy over the years?

This policy has evolved from the Comprehensive National Cybersecurity Initiative (CNCI) that was published by President George W. Bush in January 2008. The three primary tenets of the CNCI policy were:

> "To establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
>
> "To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
>
> "To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace (Bush, 2008)"

Though the Obama Administration reviewed and approved Bush's CNCI policy in May 2009, Obama, who is regarded as the most technology-savvy president that has ever occupied the White House, went much further to acknowledge the importance of cyberspace to the American economy and the American military, and the importance of defending the U.S. from adversaries that could threaten us via cyberspace. Obama's policy also acknowledges the reality that future wars will be fought on the realm of cyberspace, and has thus funded the preparation of the U.S. armed forces to prepare for conflict in cyberspace (Gerwitz, 2011).

What is the effectiveness of current policy when it concerns this particular threat issue?

The Obama Administration's policies have been effective in raising the awareness of the U.S. population as to the importance of protecting assets that are connected in cyberspace. These policies have also been effective in providing for the preparation of the U.S. military to deal with conflict in cyberspace.

However, the policies have not been particularly effective as a deterrence to cyber threats presented by potential national enemies and non-state actors. As recently as September 23, 2012 – September 30, 2012, cyber attacks in the form of distributed denial of service (DDOS) attacks from the Middle East against several major U.S. banks based have publicly demonstrated the ire of the attackers and also the vulnerabilities of banks with a customer presence in cyberspace (Strohm and Engleman, 2012).

Short-Term and Long-term Ramifications of Current Policy

In the short-term, the Obama Administration's policies regarding cyberspace have done much to raise the awareness of cyberspace as an area that requires protection for the public good and prosperity of the American people. These policies have also served to show our allies and our potential enemies that the U.S. has the intention of defending cyberspace and all our interests that are connected to it. In the long-term, these policies will probably evolve to reveal in a general, unclassified way, stronger defenses, stronger deterrent capabilities and probably offensive cyberweapons.

On the legislative front, as recently as September 23, 2012, Chairman of the Senate Homeland Security Committee, Senator Joseph Lieberman (D., Connecticut), realizing that Congress would fail to pass cybersecurity legislation to designed to help protect the United States and its people, sent an urgent letter to President Obama to ask for the creation of a new Presidential Executive Order that would address several current cybersecurity issues, that includes how and when and where law enforcement can become involved in cybersecurity issues (Kerr, 2012). Though many digital privacy rights advocates, including the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the American Civil Liberties Union have strenuously fought recent cybersecurity legislation, it is expected by many cybersecurity experts that if President Obama is reelected in November 2012, an Executive Order drafted and signed by the Obama Administration provide the tools that the federal government wants. Even if President Obama is not reelected in November 2012, it is expected that some expedient action on the part of the new president would probably take place even before Congress could successfully agree upon and pass such legislation.

Allies and Adversaries Connected to this Specific Policy?

It is entirely likely that there are classified versions of the International Strategy for Cyberspace policy that address the nature of how U.S. policies regarding the defense of cyberspace will affect our allies and our adversaries. But since it has been publicly revealed that the Obama Administration has conducted offensive cyberwarfare operations against Iran between June 2009 and June 2010, it is also likely that both our allies and our enemies have a clearer understanding of U.S. capabilities as well as the intent to use cyberweapons when it deems it is in its best interests to do so.

Conclusion

The good news is that President Obama and his Administration have an acute awareness of the importance of the cyberspace to the American economy and the American military. The bad news is that because we are already in some form of cyberwarfare that appears to be rapidly escalating, it remains to be seen what effects these cyberattacks and the expected forthcoming Executive Orders that address cybersecurity will have on the American people and our way of life. I believe it will be necessary to act prudently, carefully balancing our freedoms with our need for security, and also considering the importance of enabling and protecting the prosperity of the now electronically connected, free enterprise economy that makes the U.S. the envy of and the model for the rest of the world.

References

Andress, J. and Winterfeld, S. (2011). Cyber Warfare: Techniques and Tools for Security Practitioners. Boston, MA: Syngress.

Andreasson, K. (ed.). (2012). Cybersecurity: Public Sector Threats and Responses. Boca Raton, FL: CRC Press.

Bush, G. W. (2008). Comprehensive National Cybersecurity Initiative (CNCI). Published by the White House January 2008. Retrieved from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative on January 5, 2012.

Bousquet, A. (2009). The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York, NY: Columbia University Press.

Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.

Clarke, R. A. and Knake, R. K. (2010). Cyberwar: the Next Threat to National Security and What to Do About It. New York, NY: HarperCollins Publishers.

Czosseck, C. and Geers, K. (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.

Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf on September 30, 2012.

Freedman, L. (2003). The Evolution of Nuclear Strategy. New York, NY: Palgrave Macmillian.

Gerwitz, D. (2011). The Obama Cyberdoctrine: tweet softly, but carry a big stick. An article published at Zdnet.com on May 17, 2011. Retrieved from

http://www.zdnet.com/blog/government/the-obama-cyberdoctrine-tweet-softly-but-carry-a-big-stick/10400 on September 25, 2012.

Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.

Kaplan, F. (1983), The Wizards of Armageddon: The Untold Story of a Small Group of Men Who Have Devised the Plans and Shaped the Policies on How to Use the Bomb. Stanford, CA: Stanford University Press.

Kerr, D. (2012). Senator urges Obama to issue 'cybersecurity' executive order. An article published at Cnet.com on September 24, 2012 Retrieved from http://news.cnet.com/8301-1009_3-57519484-83/senator-urges-obama-to-issue-cybersecurity-executive-order/ on September 26, 2012.

Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.

Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.

Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all on June 28, 2009.

McBrie, J. M. (2007). THE BUSH DOCTRINE: SHIFTING POSITION AND CLOSING THE STANCE. A scholarly paper published by the USAWC STRATEGY RESEARCH PROJECT. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA423774 on September 30, 2012.

Obama, B. H. (2012). Defense Strategic Guidance 2012 - Sustaining Global Leadership: Priorities for 21st Century Defense. Published January 3, 2012. Retrieved from http://www.defense.gov/news/Defense_Strategic_Guidance.pdf on January 5, 2012.

Obama, B.H. (2011). INTERNATIONAL STRATEGY for Cyberspace. Published by the White House on May 16, 2011. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf on May 16, 2011.

Radcliff, D. (2012). Cyber cold war: Espionage and warfare. An article published in SC Magazine, September 4, 2012. Retrieved from http://www.scmagazine.com/cyber-cold-war-espionage-and-warfare/article/254627/ on September 7, 2012.

Sanger, D. E. (2012). Confront and Conceal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.

Stiennon, R. (2010). Surviving Cyber War. Lanham, MA: Government Institutes.

Strohm, C. and Engleman, E. (2012). Cyber Attacks on U.S. Banks Expose Vulnerabilities. An article published at BusinessWeek..com on September 28, 2012 Retrieved from http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability on September 30, 2012.

Technolytics. (2011). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict. Purchased and downloaded from Amazon.com on April 16, 2011.

Waters, G. (2008). Australia and Cyber-Warfare. Canberra, Australia: ANU E Press.