Week 10 – Writing Assignment

William Slater

DET 630 – Cyberwarfare and Cyberdeterrence

Bellevue University

A Brief Analysis of Cyber Challenge Symposium 5: Cyber Deterrence: "Cyber Deterrence: Mutual Assured Disruption or Other Options?" - The Potomac Institute for Policy Studies

Matthew Crosston, Ph.D. - Professor

November 4, 2012

A Brief Analysis of Cyber Challenge Symposium 5: Cyber Deterrence

In July 2011, the Potomoc Institute for Policy Studies held a Symposium on current cyber deterrence issues that face the United States, its military and its national leadership. The The panel featured Gen. Michael Hayden, USAF (Ret.), currently a Principal at the Chertoff Group and a former Director of the CIA and NSA; Michael Tiffany, Chief Architect at Recursion Ventures; and Dr. James Mulvenon, Vice President, Intelligence Division, Defense Group, Inc (Potomoc Institute of Policy Studies, 2011).

Key issues discussed during this symposium included:

1) The cyber domain is and will continue to become more and more offensive in the area of cyberweapons and aggressive actions (Delex Systems, Inc., 2011).
2) The Chinese cyber vulnerabilities are on the rise but the unique nature of their state-controlled technical infrastructure as well as some of their irregular techniques provides them with certain strategic and tactical advantages in the on the battlefield of cyberspace (Delex Systems, Inc., 2011).
3) It is conceivable that any entity endorsing the use of “mitigative counter-strikes” by individuals, corporations, and / or governments “could reduce cyber threats and deter action (Delex Systems, Inc., 2011).

Surprises and Subtleties

For me, there were both surprises and subtleties during this video. Among them:

1) Attribution is harder and so is retaliation, especially because everything related to the evidence of an attack can be faked (Potomoc Institute of Policy Studies, 2011).
2) Denial of service by proxy, such as DDoS attacks by remotely controlled zombie computers is a tremendously cheap force multiplier, making it a very compelling tool as an offensive cyberweapon (Potomoc Institute of Policy Studies, 2011).
3) How Big Is the Cyberwar and Cyber Deterrence Problem? It is the biggest thing since European man discovering the Western Hemisphere a little over 500 years ago (Potomoc Institute of Policy Studies, 2011).
4) The ability to have private hackers, like a corporate corps of deniable employees, to perform offensive cyber operations, is not that different than 18th century privateers, and the present climate is conducive to such capabilities, though the need for privateers eventually dissolved (Potomoc Institute of Policy Studies, 2011).

Conclusions

Seeing this video about cyber deterrence, as well as reviewing other sources on the topic, The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability (Gompert and Saunders, 2011) and Cyberdeterrence and Cyberwar (Libicki, 2009), led me to the conclusion that the Chinese realize the risks and the dangers of an all-out cyber war with the United States. I am not exactly sure if the Russians could be trusted to be that reasonable, but I believe that they have the sophistication to understand and appreciate the dangers of a cyber war. In the strictest sense of the word, I do not believe that the Russians or the Chinese will ever be

"allies" on the battlefield, but I believe that they may join with the U.S. to create an environment in cyberspace that rewards cooperation and punishes destructive behaviors.

Perhaps it seems a bit naïve, but I still believe that a strongly worded, explicit U.S. national policy regarding cyber deterrence would serve to further strengthen the U.S. in cyberspace as well as protect critical infrastructure and our allies. According to a 1997 paper that was prepared by the U.S. Army for the Clinton administration, ***Toward Deterrence in the Cyber Dimension: A Report to the President's Commission on Critical Infrastructure Protection***, these would be the three recommended elements of such a policy:

1) Continue to design, create, possess, and use offensive cyber warfare capabilities when necessary
2) Develop a defensive system for surveillance, assessment, and warning of a cyber attack. (I think such capability presently exists now)
3) A declaration that any act of deliberate information warfare resulting in the loss of life or significant destruction of property will be met with a devastating response (U.S. Army, 1997).

To this recipe for a strong national cyber deterrence policy, it may also be prudent to include the Crosston's idea of Mutually Assured Debilitation, that is if that message has not already heard loud and clear by the Chinese and Russian cyber warriors who would seek to do us real harm (Crosston, 2011).

References

Crosston, M. (2011). World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. An article published in the Strategic Studies Quarterly, Spring 2011. Retrieved from http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf on October 10, 2012.

Delex Systems, Inc. (2011). Consulting, Studies, and Analysis: Current Issues Brief No. 37: A review of "Cyber Deterrence: Mutual Assured Disruption or Other Options?" (7 July 2011) Retrieved from http://www.delex.com/pub/cib/Current%20Issues%20Brief%2037-Potomac%20Institute%20on%20Cyber%20Deterrence%20[Read-Only]%20[Compatibility%20Mode].pdf on November 3, 2012.

Gompert, D, C. and Saunders, P. C. (2011). The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability. National Defense University Press. Retrieved from http://www.ndu.edu/press/lib/pdf/books/paradox-of-power/paradox-of-power.pdf on November 3, 2012.

Gompert, D, C. and Saunders, P. C. (2012). Sino-American Strategic Restraint in an Age of Vulnerability. Retrieved from http://www.ndu.edu/press/lib/pdf/StrForum/SF-273.pdf on November 3, 2012.

Lan, T., et al. (2010). Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway. A technical policy paper published by the East West Institute. Retreived from http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf on November 3, 2012.

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

National Security Council, White House. (2011). The Comprehensive National Cybersecurity Initiative (CNCI). Published by the White House May 2011. Retrieved from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative on May 19, 2011.

The Potomac Institute for Policy Studies. (2011). Cyber Challenge Symposium 5: Cyber Deterrence: "Cyber Deterrence: Mutual Assured Disruption or Other Options?" (7 July 2011). Retrieved from http://www.youtube.com/watch?v=8m-GUAemkBg on November 3, 2012.

Turzanski, E. and Husick, L. (2012). "Why Cyber Pearl Harbor Won't Be Like Pearl Harbor At All..." A webinar presentation held by the Foreign Policy Research Institute (FPRI) on October 24, 2012. Retrieved from http://www.fpri.org/multimedia/2012/20121024.webinar.cyberwar.html on October 25, 2012.

U.S. Army. (1997). Toward Deterrence in the Cyber Dimension: A Report to the President's Commission on Critical Infrastructure Protection. Retrieved from http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf on November 3, 2012.