Week 03 – Writing Assignment 01

William Slater

DET 630 – Cyberwarfare and Cyberdeterrence

Bellevue University

Threat Assessment in Cyberwarfare and Cyberdeterrence

Matthew Crosston, Ph.D. - Professor

September 16, 2012

Threat Assessment in Cyberwarfare and Cyberdeterrence

One of the main disadvantages of the hyper-connected world of the 21st century is the very real danger that countries, organizations, and people who use networks computer resources connected to the Internet face because they are at risk of cyberattacks that could result in anything ranging from denial service, to espionage, theft of confidential data, destruction of data, and/or destruction of systems and services. As a recognition of these dangers, the national leaders and military of most modern countries have now recognized that the potential and likely eventuality of cyberwar is very real and many are preparing to counter the threats of cyberwar with modern technological tools using strategies and tactics under a framework of cyberdeterrence, with which they can deter the potential attacks associated with cyberwarfare.

A Single Integrated Operational Plan for War

During the 1950s and 1960s, when it became evident that nuclear weapons could play a major role in strategic warfare, the United States, utilized a think-tank of individuals, both military and civilian, to craft the strategic war-fighting plans of the U.S. that would deal with very real possibility that tactical and possibly strategic nuclear weapons may be required during a major wartime scenario. The first such war plan was called the Single Integrated Operational Plan (SIOP). The process of its creation involved the use of intelligence data about potential enemies, a threat assessment process, and then a process whereby the identified likely targets would be prioritized and matched with weapons. The process of matching weapons to targets also included intricate sequence timings, and the various event triggers that would result in the execution of such attacks. In the 1980s, the SIOP evolved into something called the OPSPLAN

and later, it was renamed the CONOPS Plan, but it has always been kept up to date and tested at least semiannually so that all involved would know their roles if the nation command authorities deemed it necessary to execute this intricate war plan.

Note that as far back as the 1970s, there were 24 defined levels of conflict between the U.S. and a potential adversary, ranging from a war of words, all the way to strategic nuclear war. No matter what the name of it was, the national war plan has always been a key tool of the national command authorities for understanding what military responses would be required in the event of these various levels of conflict.

What is the nature of the threat you have chosen?

During my studies prior to and as a student in this DET 630 – Cyberwarfare and Cyberdeterrence course at Bellevue University, it occurred to me that considering the rapid evolution of the potentially destructive capabilities of cyberweapons and the complex nature of cyberdeterrence in the 21st century, it is now a critical priority to integrate the cyberwarfare and cyberdeterrence plans into the CONOPS plan. Indeed, if the strategic battleground of the 21st century has now expanded to include cyberspace, and the U.S. has in the last five years ramped up major military commands, training, personnel, and capabilities to support cyberwarfare and cyberdeterrence capabilities, the inclusion of these capabilities should now be a critical priority of the Obama administration if has not already happened.

How large a problem is this for the United States?

Without the integration of cyberwarfare and cyberdeterrence technologies, strategies, and tactics into the CONOPS Plan, the national command authorities run a grave risk of conducting a

poorly planned offensive cyberwarfare operation that could precipitate a global crisis, impair relationships with its allies, and potentially unleash a whole host of unintended negative and potentially catastrophic consequences. In non-military terms, at least four notable cyberspace events caused widespread damages via the Internet because of the rapid speed of their propagation, and their apparently ruthless and indiscriminant selection of vulnerable targets. They are 1) the Robert Morris worm (U.S. origin,1988); 2) the ILOVEYOU worm (Philippines origin, 2000); the Code Red worm (U.S. origin, 2001); and the SQL Slammer worm (U.S. origin, 2003). If not executed with great care and forethought, a cyberweapons could potentially unleash even greater damage on intended targets and possible on unintended targets that were connected via the Internet.

Other Not So Obvious Challenges for Cyberweapons and Cyberdeterrence

The cyberspace threat and vulnerability landscape is notable in that it is continually dynamic and shifting. Those who are responsible for protecting assets in cyberspace have many more challenges on their hands than their military counterparts who utilize weapons like guns, explosives, artillery, missiles, etc. For example, there are by some estimates over 350 new types of malware that are manufactured each month. There are also monthly patch updates to most Microsoft software and operating systems, and phenomena such as evil hackers and zero-day exploits are apparently never ending. Therefore, the inclusion of cyberweapons and cyberdeterrence capabilities into the CONOPS Plan would require more frequent, rigorous, complex, and integrated testing to ensure that it was always effective and up to date. In the dynamic world of cyberspace with its constantly shifting landscape of new capabilities, threats

and vulnerabilities, the coordination of the constant refresh and testing of a CONOPS Plan that integrated these cyberwarfare and cyberdeterrence capabilities would be no small feat. In addition, constant intelligence gathering and reconnaissance would need to be performed on suspected enemies to ensure that our cyberweapons and cyberdeterrence capabilities would be in constant state of being able to deliver the intended effects for which they were designed.

Is it a problem for other countries?

The careful planning and integration of cyberweapons and cyberdeterrence is likely a challenge for every country with these capabilities. For example, much is already known about our potential adversaries, such as Russia, China and North Korea, but what is perhaps less understood is the degree to which they have been successful in integrating cyberwarfare and cyberdeterrence capabilities into their own national war plans. Nevertheless, due to the previous extensive experience of Russia and the U.S. with strategic war planning, it is more likely that each of these countries stand the greatest chance of making integrating cyberwarfare and cyberdeterrence capabilities into their respective war plans. Yet, as far back as June 2009, it was clear that the U.S. and Russia were unable to agree on a treaty that would create the terms under which cyberwarfare operations could and would be conducted (Markoff, J. and Kramer, A. E., 2009).

Is it problematic for these countries in the same ways or is there variation? What kind?

Every country that is modern enough to have organizations, people, and assets that are connected to computers and the Internet faces similar challenges of planning and managing cyberweapons and cyberdeterrence, and the poorer the country, the more significant the

challenges. For example, when a small group of hackers from Manila in the Philippines unleashed the ILOVEYOU worm on the Internet in 2000, it caused over $2 billion in damages to computer data throughout the world. Agents from the FBI went to Manila to track down these people and investigate how and why the ILOVEYOU worm catastrophe occurred. To their surprise, they learned that each of these hackers who were involved could successfully escape prosecution because there were no laws in the Philippines with which to prosecute them. So actually most countries lack the technological and legal frameworks with which to successfully build a coordinated effort to manage the weapons and strategies of cyberwarfare and cyberdeterrence, despite the fact that most now embrace cyberspace with all the positive economic benefits it offers for commerce and communications.

What are the consequences to the U.S. and others if this threat is left unchecked?

As stated earlier, without the careful integration of cyberwarfare and cyberdeterrence technologies, strategies, and tactics into the CONOPS Plan, the national command authorities run a grave risk of launching a poorly planned offensive cyberwarfare operation that could precipitate a global crisis, impair relationships with its allies, and potentially unleash a whole host of unintended negative and potentially catastrophic consequences.

What consequences has the threat already produced on American/global society?

I believe that yes, the absence of well-defined cyberwarfare and cyberdeterrence strategies and tactics in the CONOPS Plan has already produced some situations that have either damaged America's image abroad, or that could imperil its image and have far more negative

consequences. For example, operates such as Stuxnet, Flame, Duque, etc., might have either been better planned or possibly not executed at all if cyberwarfare and cyberdeterrence strategies and tactics were defined in the CONOPS Plan. Also, the news media indicated during the revolution in Libya that resulted in the fall of Qaddafi, cyberwarfare operations were considered by the Obama administration. The negative reactions and repercussions on the world stage might have far outweighed any short term advantages that could have resulted from a successful set of cyberattacks against Libyan infrastructure assets that were attached to computer networks. Again, a comprehensive CONOPS Plan that included well-defined cyberwarfare and cyberdeterrence strategies and tactics could have prevented such possible cyberattacks from even being considered, and it could have prevented the news of the possible consideration being publicized in the press (Schmitt, E. and Shanker, T., 2011). Without such restraint and well-planned deliberate actions, the U.S. runs the risk of appearing like the well-equipped cyberbully on the world stage, and an adversary who is willing to unleash weapons that can and will do crippling damage to an opponent, using technologies that are rapid, decisive, and not well-understood by those for whom they are intended. A similar effect and world reaction might be if U.S. Army infantry troops were equipped with laser rifles that emitted deadly laser blasts with pinpoint precision across several hundred yards.

Has this threat evolved or changed over time or is it relatively constant? If it has evolved or changed, exactly how has that change happened and what political consequences have emerged from them?

The threat has certainly rapidly evolved over time. Since Stuxnet was released in 2010, countries and the general public are now aware of some of the offensive, strategic and destructive capabilities and potential of cyberweapons (Gelton, T., 2011).

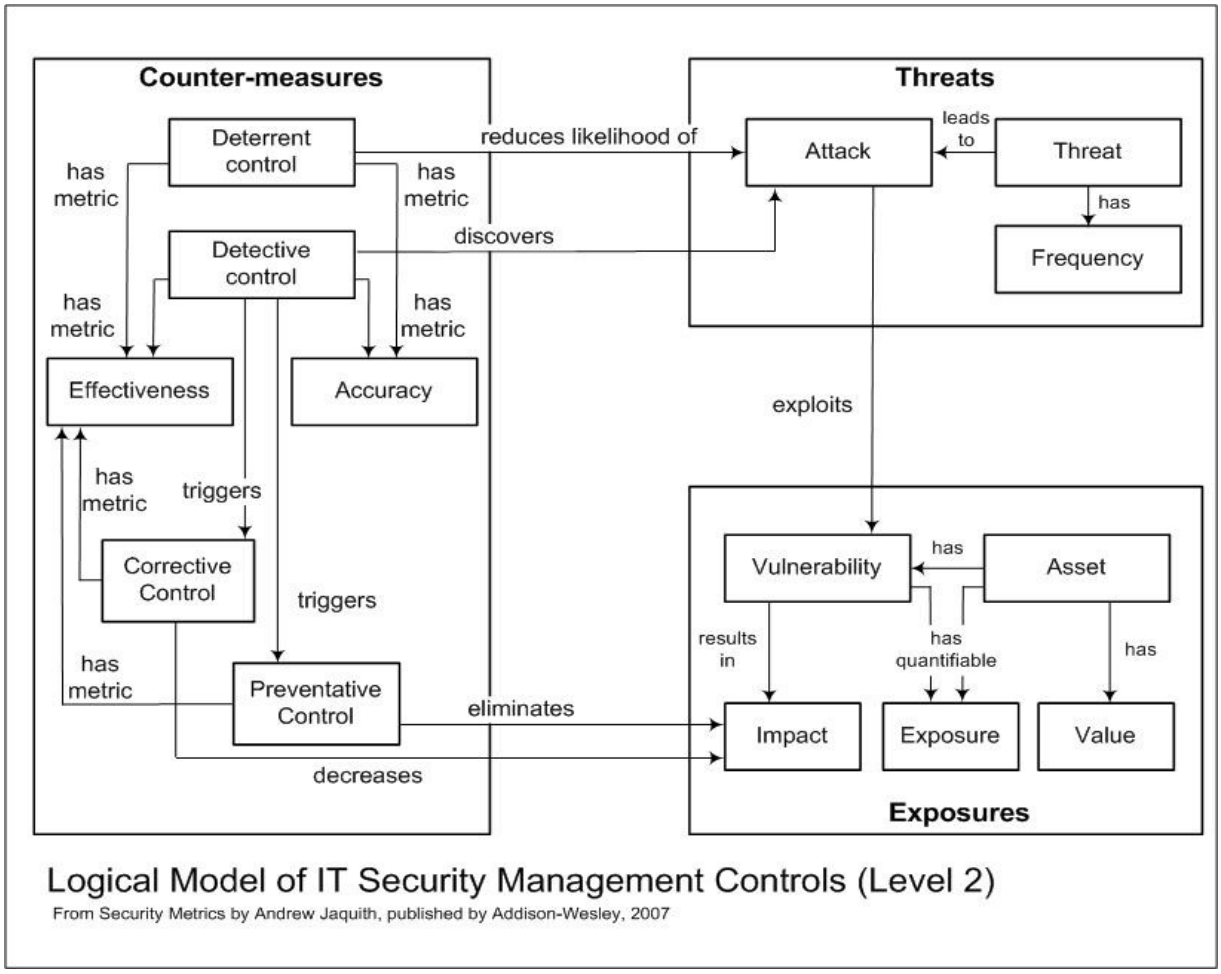
The changes that produced Stuxnet and other recent, more modern cyberweapons were a national resolve to excel in the cyberwarfare area, coupled with excellent reconnaissance on desired targets, and partnering with computer scientists in Israel. The political consequences are not well understood yet, except to say that the U.S. and Israel are probably less trusted and suspected of even greater future capabilities, as well as having the will to use them. Again, having well-planned cyberwarfare and cyberdeterrence strategies and tactics defined in the CONOPS Plan might indeed, restrain such possibly reckless decisions as to unleash cyberweapon attacks without what the world might consider the correct provocation.

Final Thoughts about Cyberwarfare Operations

In the words of Deb Radcliff, in an article published in SC Magazine in September 2012, "we are already in a cyberwar" (Radcliff, D., 2012). But as I was performing my research, it occurred to me that a country like the U.S., might in the future unleash such a devastating cyberattack that it could cripple the enemy's ability to communicate a surrender. I think that the moral implications of such circumstances need to be justly considered as a matter of the laws of war, because if a country continues to attack an enemy that has indicated that they are defeated

and want to surrender, this shifts the moral ground from which the U.S. may have it was conducting its cyberwarfare operations. This is one other unintended consequence of cyberwarfare and one that needs to be carefully considered.

To further understand the relationship of threats, counter-measures, and exposures in cyberspace, I have included this diagram by Jaquith, shown below.



Logical Model of IT Security Management Controls (Level 2)

From Security Metrics by Andrew Jaquith, published by Addison-Wesley, 2007

References

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

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

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: HaperCollins Publishers.

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

Edwards, M. and Stauffer, T. (2008). Control System Security Assessments. A technical paper presented at the 2008 Automation Summit – A Users Conference, in Chicago. Retreived from http://www.infracritical.com/papers/nstb-2481.pdf on December 20, 2011.

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

Friedman, G. (2004). America's Secret War: Inside the Hidden Worldwide Struggle Between America and Its Enemies. New York, NY: Broadway Books.

Gjelten, T. (2010). Are 'Stuxnet' Worm Attacks Cyberwarfare? An article published at NPR.org on October 1, 2011. Retrieved from

http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet on December 20, 2011.

Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from http://www.npr.org/templates/story/story.php?storyId=130260413 on December 20, 2011.

Gjelten, T. (2011). Security Expert: U.S. 'Leading Force' Behind Stuxnet. An article published at NPR.org on September 26, 2011. Retrieved from http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet on December 20, 2011.

Gjelten, T. (2011). Stuxnet Raises 'Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011.

Grabo, C. M. (2004). Anticipating Surprise: Analysis for Strategic Warning. Lanham, MD: University Press of America, Inc.

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

Jaquith, A. (2007). Security Metrics. Boston, MA: Addison Wesley.

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.

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

Langer, R. (2010). Retrieved from http://www.langner.com/en/blog/page/6/ on December 20, 2011.

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.

Payne, K. B. (2001). The Fallacies of Cold War Deterrence and a New Direction. Lexington, KY: The University of Kentucky Press.

Pry, P. V. (1999). War Scare: Russia and America on the Nuclear Brink. Westport, CT: Praeger Publications.

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.

Retrieved from http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar on December 20, 2011.

Reynolds, G. W. (2012). Ethics in Information Tehnology, 4th edition. Boston, MA: Course Technology.

Rosenbaum, R. (2011). How the End Begins: The Road to a Nuclear World War III. New York, NY: Simon and Schuster.

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

Schell, B. H., et al. (2002). The Hacking of America: Who's Doing It, Why, and How. Westport, CT: Quorum Press.

Schmidt, H. S. (2006). Patrolling Cyberspace: Lessons Learned from Lifetime in Data Security. N. Potomoc, MD: Larstan Publishing, Inc.

Schmitt, E. and Shanker, T. (2011). U.S. Debated Cyberwarfare in Attack Plan on Libya. An article published in the New York Times on October 17, 2011. Retrieved from http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html on October 17, 2011.

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

Swiderski, F. and Snyder, W. (2004). Threat Modeling. Redmond, WA. Microsoft Press.

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.

Wikipedia Commons. (2011). Stuxnet Diagram. Retrieved from http://en.wikipedia.org/wiki/File:Step7_communicating_with_plc.svg on December 20, 2011.

Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. An article published on July 11, 2011 at Wired.com. Retreived from http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 on December 20, 2011.