Matthew Boeck
11/8/2011
SE4930
Dr. Schilling

Article Review #1 – Cyberwarfare

The article that I read was about Cyberwarfare and can be found at http://www.computer.org/csdl/mags/sp/2011/05/msp2011050013.html. This article was written in September/October 2011 and is Vol. 9, No.5. It was pages 13-15 and was published by the IEEE Computer Society and written by Thomas A Berson of Anagram Laboratories and Dorothy E. Denning of Naval Postgraduate School. This article began by talking about how cyberspace can be used to facilitate three types of conflict. It can be a source of conflict, a tool of conflict, or a target of conflict. This article focuses on how cyberspace can be a subject to cyber attacks and how cyber attacks can be an instrument of warfare leading to cyberwarfare.

The article then talks about the different types of cyber attacks going back to a protest against nuclear weapons in 1989. It is interesting to see that people (governments and the private sector) have been writing malicious software or using software for malicious means since the early 1990s! The article gives many sources for more information on this topic. One of the things I learned from reading this article is that in several instances, a physical act of war (like an accidental bombing) lead to cyber attacks. For example, Chinese hackers defaced US websites because their embassy in Belgrade was accidently destroyed by US airstrikes. This is just one example the article mentions.

I also saw something about Stuxnet. This is an area that I have been studying immensely in the last few months. I find this very interesting. Essentially, this malware was written to target the SCADA (supervisory control and data acquisition) systems of Iran's nuclear enrichment facility. This malware caused turbines to spin too fast, not report errors, and essentially break themselves by running too long or too fast. What is most interesting about this topic, is that nobody knows where the malware came from or who wrote it. Because Stuxnet had 4 zero-day vulnerabilities built into it (this is incredibly rare and sophisticated) as an attempt to ensure exploitation, many people think high-class research or government organizations had to have written it, because it would be far too much work for a group of hackers to write.

Because of the field I currently work in, (IT Security for a company) I have to be very conscious of emerging threats, especially when it comes to cyber attacks and cyber warfare. The company I work for can be considered a high-value target, to the point that we need to monitor social networks for emerging threats against us. From this article I learned that it isn't necessarily underground "hacktivists" that we need to be worried about, but even other governments. I also learned that the software you write can not only be targeted for attacks, but can be *used* as a tool for attacks. I currently develop software for this company, and I will be more cautious of the security implications behind the code. I am already aware of the CIP (critical infrastructure protection) requirements the software will need to meet, but I also need to be aware of who uses the software, and will need to ensure that only those authorized people are using it.

One of the questions I had from reading this article is what are governments doing to protect against cyber attacks and cyberwarfare? I know that underground organizations as well as government sectors are beginning to use technology as a means for warfare, but what are governments doing to protect against it? Are we building special units to analyze code, dissect malware, research emerging trends, or are we taking a more reactive rather than proactive approach?