Nathan Dykstra
SE 4930
Article Review 1
December 14, 2011

Article Choice

I read the article *Cybermilitias and Polticial Hackers* by Scott D. Applegate from the September/October 2011 issue of Security & Privacy.

What Was Discussed

This article covered the topic of cyberwarfare and, more specifically, its implications as an actual act of war or aggression as outlined by the United Nations charter. The author uses the examples of Russia's cyber attacks on Georgia and Estonia and China's repeated offenses throughout recent years to illustrate some patterns and problems with these scenarios.

When Georgia was fighting Russia for sovereignty, a series of cyber attacks were launched from within Russia that crippled many Georgian government and media web sites directly before Russia launched a ground offensive. Many experts don't see this as a coincidence, but due the anonymous nature of the Internet, there is no direct evidence linking the Russian government to these activities.

This anonymity is the same reason why no direct links to China have been established for any attacks originating from that country. The author explains how China has quite a long track record of cyber attacks but no action has been taken against them. Many of these attacks are attributed to politically motivated hacker groups unaffiliated with the government.

Indeed, many countries place the blame of cyberwarfare attacks on such groups. Again, because of the anonymous nature of the Internet, no direct links can be made to the governments of these instigating nations.

A serious problem, as Mr. Applegate points out, is the the United Nations charter lacks a valid description for cyberwarfare. Since this definition does not exist, these activities can not be considered lawful acts of aggression by the instigating nation warranting repercussions from other bodies. The U.N. defines acts of aggression as "the use of armed force by a State against

the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations." The author points out that the main problem with this statement is the "armed force" phrase. He goes on to question what constitutes an armed force, as many militaries consider computers weapons of warfare. This is followed by a line of questioning including: if computers are considered weapons, are hackers considered combatants? and what benefits/detriments do nations receive by maintaining a hacker force?

What I Learned

I think the main thing I gathered from this article was how important definitions are in the field of cybersecurity, especially relating to international relations. I also learned how aggressively China is pursuing cyber attacks as the author mentions the many related books and articles that are published there and the overt organizations that the People's Army (not to mention the covert groups). Lastly, I found that we could be dangerously close to fighting a war with a nation that is accused of harboring hackers; the author made the analogy of America's invasion of Afghanistan for harboring terrorists.

How It Will Help

This article and the information therein will help me better understand how current cyberattacks are performed and why they are so difficult to track. I can also use the knowledge of these cyberattacks and there effects to realize that the complexity of the systems involved may have unintended repercussions.

Questions

If a computer is a weapon, does that mean I can't bring my laptop to school?
We hear of other nations' cyberattacks, what kind has America instigated?

Nathan Dykstra
SE 4930
Article Review 1
December 14, 2011

What tools can we use to better track/mitigate cyber attacks from foreign nations?

What about cyber attacks from within the nation?