The Hand book of information and Cyber Ethic

Chapter14: The ethics of cyber conflict

Amazonlink:

http://www.amazon.com/Handbook-Information-Computer-Ethics/dp/0471799599/ref=sr_1_1?ie=UTF8&s=books&qid=1233037513&sr=1-1

What I expect to learn:

- To learn more about the cyberspace
- To learn the ethics of cyber conflict
- To learn about the different cyber attacks in the past

Quote:

> "Besides cyber attacks conducted for pleasure or personal gain, the paper does not consider revenge attacks by insiders – all of which are generally regarded as unethical."

Book Review:

The issue of law and cyber conflict is something that while relatively new, is something that people, nation states, and military organizations have been working on for the last 10 years at least. Many countries have robust cyber warfare rules of engagement, and the more interesting part about this is that any country with an internet connection can engage in cyber conflicts. Attribution (IE Knowing who is attacking you, and being able to act appropriately against the real place that is attacking you) has long been a problem. Zombies, bot nets, jump points, and the millions of compromised computers both Windows and Linux are the cannon fodder of cyber warfare. Attributing the attacker back to the point of origin is going to be difficult if not impossible without some smart people having unrestricted access to packets, and to compromised systems. Legally though, it gets more interesting as the state of cyber law is often well behind the state of cyber warfare tools.

With the advancing technology, even internet can cause war to countries. It could be a silent war; no one would get hurt… physically. Cyber conflict may result to chaos to the concerned parties. Such as what happened in September 2000, wherein Israelite teenage hackers created a website that successfully jammed six websites in Lebanon, causing a huge turmoil in different websites in Israel, including those of the Palestinians and at least one U.S. site. They made two main types of attacks, the website defacement and distributed denial of service.

What I have learned:

- Jus ad bellum – the law of conflict management
- Jus in bello – the law of war
- Distinction of combatants from non combatants
- When does cyber attack constitute the use of force

Integrative Question:

1. What is cyberspace?
2. What is hacktivism?
3. What happened in the law of war?
4. What is the doctrine of self defense?
5. What is hack back and force?