DEBATE

Debate Topic: Cyber War

Faculty Name: Mr. Sanjay Kumar Nayak

Debate Date: 18/03/2017

SUMMARY

We are in the early years of a cyber war arms race and we are going to see much more of that in the future. Countries like North Korea have a natural advantage in this type of cyber warfare, he warned, because of the basic level of technical infrastructure that they possess. North Korea has natural cyber-defenses in that it only has about 1,000 IP addresses, and it has only very few computers so its 'terrain' is very defensible. By contrast the U.S. is extremely vulnerable because it has lots of computers and Internet infrastructure.

Cyber warfare involves the use and targeting of computers and networks in warfare. It involves both offensive and defensive operations pertaining to the threat of cyber attacks, espionage and sabotage. There has been controversy over whether such operations can duly be called "war". Nevertheless, nations have been developing their capabilities and engaged in cyber warfare either as an aggressor, defendant, or both.

Cyber warfare has been defined as “actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption”, but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations.

Cyber Attacks and Why Attribution Matters

In addition, some cyber warfare attacks may be carried out by groups (such as terrorist organizations) rather than countries. Just as it is hard to fight an unknown enemy in real life, it is hard to react to unknown attackers. We are living in a world now where we can be attacked and not know if the attacker is a foreign government or just a couple of guys or others. Someone said. “Technology is spreading capabilities, and the same weapons and tactics are available to everyone”.

This difficulty with attribution is valuable for attackers, because without attribution it is impossible to retaliate. The ability to carry out attribution is therefore a deterrent to would-be attackers.

There are four types of Cyber Attacks

- **High focus, high skilled attacks:** These are the advanced persistent threats that present the biggest danger to every organization
- **Low skill, high focus attacks:** These targeted attacks can be beaten by good security measures which are too effective for the attacker to overcome
- **Low focus, high skill attacks:** These involve identity theft and credit card breaches, which require good security to defend against
- **Low focus, low skill attacks:** These are generally carried out by script kiddies, and organizations should be able to keep them out without too much difficulty

To defend against low focus attacks you just need to be more secure than the guy next to you. With highly focused attacks this relative security is irrelevant; your security has to beat the attacker's skill. With a high focus, high skill attack, a sufficiently skilled attacker will always get in. We are all vulnerable.

Without the ability to attribute attacks, It is also impossible to distinguish between computer network exploitation, a classic data breach where an attacker exploits vulnerabilities to steal things, and computer network attacks, where the attacker's motivation is to cause damage. It's the difference between copy and delete.

“Cyber war is like a hell and it will be worse in future.”