Forum: General Assembly 1

Issue: Cyber security and the protection against cyber warfare

Student Officer: Tom Lee

Position: President of the General Assembly 1

Introduction

As technology develops, humanity's reliance on technology rapidly increases. People's lives have reached the point where absence of technology can greatly damage the fluency of their lives. Among the variety of technology people utilize, network is one of the major technological improvement that brought convenience to people's lives; this technology allows electronic devices to share information and resources. A well-known example of a network is the internet. Individuals use network for simple tasks such as messaging their friends or googling for information. Companies use network to internally share various resources or to save their consumer's personal information. Governments use network to keep record of their citizens' information or to save classified information.

However, this prevalent usage of network has created a breeding ground for crime and attacks that threaten the safety of individuals, companies, and even governments. Ever since the creation of network, "hackers" have anonymously threatened users in the cyberspace, utilizing various methods; also, countries have assembled cyber attack forces to launch attacks on networks of other countries' important facilities, starting cyber warfare between countries. These malicious occurrences placed emphasis on the need for cyber security and protection against cyber warfare.

Definition of Key Terms

Network

Network is a platform where users can share resources and data through direct or wireless connections.

Hacking

Hacking is often referred as an unwarranted intrusion to a network or a system. The hacker might hack the system or network to steal information, damage the website, or terrorize civilians.

Backdoor

Backdoor is a secret and illegitimate way of passing through the existing security authentication.

Denial of Service attack

Denial of Service attacks, commonly known as DoS, is a cybercrime that makes devices or networks temporarily or permanently inaccessible.

Distributed Denial of Service attack

Distributed Denial of Service attacks, commonly known as DDoS, is similar to DoS, but the attacker utilizes another individual's computer, known as zombies, to launch massive DoS attacks on high profile websites.

Direct Access attack

Direct Access attack is when an user directly connects to the network or the system to conduct the cyber attack. Through direct access, the user can easily comprise the existing security.

Spoofing

Spoofing is stealing private information by imitating an authorized source.

Eavesdropping

Eavesdropping is secretly listening or viewing a private conservation in order to steal information or supervise a potential threat.

Background Information

Origin

When networks were created, cyber security was not a serious or a concerning issue as hacking was only done through direct access. However, as time passed, hackers developed a variety of viruses and techniques to steal information or damage the system. It was not possible for users to protect themselves in cyberspace with the existing simple methods of protection, and this resulted in the large increase in demand for a proper cyber security against the malicious codes sent by hackers. As various hacking methods were developed by black hackers, white hackers simultaneously developed cyber security programs to protect users and their networks from being exposed or damaged by these malicious codes.

What is Cyber Warfare?

Cyber warfare is action conducted by a nation in cyberspace against another nation to cause damage or disruption to their networks or system. Many nations have an official cyber response team, and they have a surreptitious cyber attack team. Cyber warfare might also be caused by terrorist groups, hacking groups, or political extremist groups. Usually, threat of cyber warfare is classified into 3 different categories: Cyber attack, Cyber espionage, and propaganda

Cyber attack is when the a nation's system is directly attacked by another hacking group. Usually, the targets of cyber attack are important government systems as the attacker's intention is to disturb and paralyze the country.

Cyber espionage is when a nation spies on the network of another country to steal information and supervise for potential threat. Although this is not considered a cyber attack, if revealed, this creates tension between nations. This is the most common method of cyber warfare between countries.

Propaganda is when a group tries to psychologically influence an audience by altering information or spreading different ideologies. Through cyber propaganda, these groups try to instill certain opinions into the audience of the materials they hack into.

.

Key Issues

Financial system

Financial systems are a key target of hackers as it gives them a source of illicit income. Hackers often hack into financial systems to obtain private information about bank accounts, and uses that information to illegally obtain money from the bank. Furthermore, by hacking financial institutes, hackers can obtain classified information about the market, which allows them to manipulate the market and earn money.

For example, in 2017, waves of ransomware attack called the "Wannacry" were launched on various institutions (the financial institutions were one of the major targets). The hackers required money from these financial institutions in return for the locked information and data. Although ransomware was a common cyber crime, Wannacry was a significant event as hackers were able to access the information through a code that exploited a vulnerability in the Microsoft systems; strangely, the code that vulnerified microsoft software was actually designed by the United States of America's NSA.

Industrial Equipment or Services

Industrial Equipments or Services includes things such as the Electricity service, telecommunication services, and nuclear power plants. All of these services are controlled by computers, which means that they are also vulnerable to cyber attacks. These services are potential targets of hacker groups, but these services tend to have relatively weaker cyber security to protect it from possible attacks.

For example, in 2015, the Ukrainian power system was infected by a malware package called "Black Energy". If a machine was infected by this package, it was unable to boot itself, and all the data within the machine was wiped off. Furthermore, it guaranteed a secure pathway for the hackers, which meant that the proprietors could permantally control the machinery. This resulted in loss of electricity for 700,000 Ukrainians, and a great financial loss for the government as they had to recover all the loss information.

Consumer devices

Hackers tend to hack into devices of individuals to obtain their private information. These informations are usually sold to groups that abuse the identity of the person for illicit purposes. When compared to companies, consumer devices usually have weaker defense against potential threats, which indicates that it is easier for hackers to illegally access the devices.

Usually, there isn't a large scale cyber attacks on consumer devices. The hackers will usually obtain the personal information of the individual through methods such as phishing. Also, there are incidents where the information of the individual is stolen from a larger network to gain access to the individual's device or accounts.

Government

Often, cyber attacks are targeted at government agencies or services controlled by the government. Hackers try to steal classified military information and personnel record, control government infrastructure, and even eavesdrop intelligence agency communication.

For example, "Shadow Network", a computer espionage operation, was launched by China on the Indian government. It was able to infect the network of the government through malicious code implanted in social media platform. As a result, the operation successfully stole classified documents and emails, and other high-level information from the Indian government.

Timeline of Events

Date	Description of event
2 November 1988	The Morris Worm- This was the first computer virus created by Robert Morris. Without a valid cyber security system in place, the damage of this virus was massive; almost 10 billion dollars worth of damage was caused.
3 November 2003	Council of Europe Convention on Cyber Crime. This was a convention that started with the purpose of devising effective cyber security methods to protect the users and detect the malicious codes in early stages of the attack. The convention raised awareness about the gravity of cybercrime, and countries started to treat the threat of cyber attack as serious issues.
8 September 2006	The United Nations Global Counter Terrorism Strategy- This was a resolution that urged to stop all forms of terrorism, including cyber terrorism.
26 April 2007	Estonia Cyber Attack- After a minor dispute with Russia over War memorials, Estonia received a myriad of cyber attacks from an unknown source. The cyber attacks targeted government databases, banks, and even business. This was the first large scale cyber attack on a nation, and after this event, countries started to fortify their cyber security infrastructures.
June 2015	Cooperation against Cyber Crime- This is a project funded by various countries and firms to improve the existing cyber security systems.

UN Involvement, Relevant Resolutions, Treaties and Events

UN has made efforts to combat the increase in cyber attacks. They held conferences, passed resolution, and raised awareness about the issue through its different agencies. However, the effectiveness of United Nation is questionable as its effectiveness directly depends on the cooperation of countries. Almost all countries pretend that they support the UN's resolutions and decisions, but they still run their surreptitious cyber units in their countries. Relevant UN articles in this regard include:

- Combating criminal misuse of information technologies **(A/RES/55/63)**
- Combating criminal misuse of information technologies **(A/RES/56/121)**
- Creation of a global culture of cybersecurity (**A/RES/57/239)**

- Creation of a global culture of cybersecurity and the protection of critical information infrastructures(**A/RES/58/199)**

- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (**A/RES/64/211)**

Bibliography

"United Nations Launches Global Cybersecurity Index" UNITU. Web. 8th January 2018

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx

"Timeline of Computer Security Hacker History " Wikipedia. Web. 8th January 2018

https://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history

"Types of Attacks" Rapid 7. Web. 8th January 2018

https://www.rapid7.com/fundamentals/types-of-attacks/

"Cyber Attacks on Electrical Grids". Scarinci Hollenbeck .Web. 9th January 2018

https://scarincihollenbeck.com/law-firm-insights/litigation/cyber-security/cyber-attack-electric-grid

"List of Cyber Attacks". Wikipedia. Web. 9th January 2018

https://en.wikipedia.org/wiki/List_of_cyberattacks

"What is cyber attack?". CSO Online. Web. 9th January 2018

https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

"Shadow Network". Wikipedia. Web. 10th January 2018

https://en.wikipedia.org/wiki/Shadow_Network