REACTION PAPER FOR

CYBERWAR

SUBMITTED BY:

CHRISTIAN STEWART

SUBMITTED TO:

GODWIN MONSERATE

1. What is your reaction on the presentation regarding cyberwars? Cite your own opinion with facts on how cyberwar, cybercrimes and/or cyberterrorism, thrive today. 25pts

Based on what I've learned from the PowerPoint presentation on cyberwars, I was really intrigued by what was discussed. First of all, I was always curious regarding the "behind the scenes" of the online world. Academic-wise, this is the first time I've learned about such so it is quite a good experience for me to learn of such.

I believe, especially in this time and age, that cyberwar is very prominent even if we are unaware of it occurring. The best schemes are those that go undetected, so how would common folk know that they are being hacked, or their information has been stolen. We know that in the age of technology, data is king. Having information means having power. Having certain power means you are in the prime position to use it responsibly, using it for its dedicated purpose.

The presence of such data online is both a blessing and a curse. It can be used to further advance our understanding of people and improve technological processes and on the other of the spectrum, it can be used to harm individuals or even organizations when such sensitive data is not protected. These individuals are called cyber criminals.

These criminals have different intentions and also use various methods in obtaining what they want illegally and immorally. Everyday people who are unaware or illiterate to the cyberworld, easily fall victim to heinous acts schemed by these cybercriminals. These people can access your information through unsecured public Wi-Fi access points and can even capture your data when you send it across the network.

Industries that thrive in the cyberworld make it their top priority to protect the information they collect against these threats and attacks. Criminals often go for sensitive information like medical records, employment and financial records, and the like. If someone steals your National ID, you'd be very worried as this contains valuable information regarding you and can be used against you. Likewise, if your bank account information stored online has been compromised, that is a direct threat to your livelihood.

With the emergence of online technology, so does the need for cybersecurity. In the eyes of terrorism, with more technology comes more exploits to be made. This is why cybersecurity is an ever-growing field in which it must match the growth that our technology advances. With the introduction of mobile devices and the emergence of IoT (Internet of Things), the amount of information and networks that require protection has tremendously increased which also increases the urgency of better security and data protection.

Despite the increase of cybercrimes, there are professional organizations who collaborate with one another to combat these crimes. These organizations are comprised of skilled and knowledgeable individuals that have obtained professional certifications in order to protect information in the cyberworld. Even I can pursue becoming a cybersecurity specialist by committing myself to lifelong learning regarding IT and also pursue internships and ethical hacking competitions.

2. With regards to the European Convention on Cybercrime, was their conclusion substantial enough to assure and educate the IT industries, government, and the public regarding these threats? 25pts

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations (taken from Wikipedia.org). It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, Philippines, South Africa and the United States.

Back in November 23, 2001, the Convention on Cybercrime was signed and was effective on July 1, 2004. This is a treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and lawful interception.

If I were to judge such convention as if I was one of the participants of the council who drew up such treaty – I would look at it as adequate enough to deal with cyber threats. Compared to the cyberworld today, back in 2001 the Internet should be less significantly less complex and intricate. The pursuit of a common criminal policy aimed at the protection of society against cybercrime is a fairly straight forward response towards such threats. To put it into simple terms, it was a good step forward in the right direction.

Now, to judge it as someone 21 years later – in hindsight, I believe the European Convention on Cybercrime provided the foundation to combat the growing threat of global cybercrime as it was the very first world-wide approach to handling the situation. It increased international cooperation and provided an avenue for unified awareness campaigns on such cybercrimes. It also created an impending urgency for countries to become proactive and agile in developing national cybersecurity strategies and punish criminal offenses for cyber-attacks.

3. List about 5 examples of cyber malwares, determine the origin, how was it spread and the effects. 25pts

a. **Virus**

A virus is malicious executable code attached to another executable file, such as a legitimate program.

Most viruses require end-user initiation, and can activate at a specific time or date.

Some computer viruses are programmed to harm your computer by damaging programs, deleting files, or reformatting the hard drive. Others simply replicate themselves or flood a network with traffic, making it impossible to perform any internet activity.

b. **Spyware**

Is software that enables a criminal to obtain information about a user's computer activities.

Some types of spyware software are embedded inside the install packages of Internet software downloads. Spyware applications may be disguised as useful programs themselves, or they may accompany other applications as part of an integrated (bundled) installation package. Spyware software can also be installed on a computer through the download of:

- Third-party Web browser toolbars or add-ins.
- Utility programs like video players or advertising blockers.
- Packages promoted be "anti-spyware" or antivirus systems that in fact contain spyware software, sometimes called scareware.
- Other "freeware" applications.

Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings.

c. **Trojan Horse**

Is a type of malware that downloads onto a computer disguised as a legitimate program in order to deceive you into running harmful programs on your computer. A Trojan horse, by definition, is not a computer virus because it cannot duplicate itself, despite the fact that it can be disseminated to numerous computers.

The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.

d. **Logic Bomb**

Is a malicious program that is triggered when a logical condition is met, such as after a number of transactions have been processed, or on a specific date (also called a time bomb).

A logic bomb is often inserted by someone with inside knowledge of the system — such as when a disgruntled employee embeds a logic bomb in their company's network. And since they're

activated by a specific condition, logic bombs can go undetected for long periods of time, until they’re triggered by the coded condition.

When this condition is met, the logic bomb is triggered — devastating a system by corrupting data, deleting files, or clearing hard drives.

e. **Ransomware**

Is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

Threat actors must gain access to a device or network. Having access enables them to utilize the malware needed to encrypt, or lock up, your device and data. Some ways to access to a device or network can be phishing, social engineering, spam and adware.

The possible effects of ransomware can be temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.

4. Give any information pertaining to mitigation of cyber-terrorism not only in the country but the whole world? 25pts

There is a global organization dedicated to security in the information society. The United Nations Office on Drugs and Crime has an agency called the International Telecommunications Union, a premier global forum through which parties work towards consensus on a wide range of issues affecting the future direction of the ICT industry. This agency has launched the Global Cybersecurity Agenda which is a framework for international cooperation aimed at enhancing confidence and security in the virtual environment.

The ITU Global Cybersecurity Agenda identifies five strategic pillars: legal, technical, organizational, capacity-building, and cooperation. The legal pillar focuses on harmonized regulations and laws relating to cybersecurity and cyber-dependent and cyber-facilitated crimes. The technical pillar covers existing technical institutions, cybersecurity standards and protocols, and the measures needed to deal with cybersecurity threats. The organizational pillar includes organizational structures and policies on cybersecurity and responsible agencies for coordinating cybersecurity policy. The capacity-building pillar covers efforts to promote cybersecurity awareness, education and training. The cooperation pillar focuses on inter-agency and public-private partnerships, information sharing networks, and cooperative agreements.

Another organization called the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) developed a comprehensive framework to guide information security management. They create information security standards and even though the standards are not mandatory, most countries use them as a de facto framework for implementing information security.

Another example of cyberterrorism mitigation is the ISACA group track law enacted related to cyber security which address personal privacy and intellectual property. Although laws may vary from country to country, these laws can serve as foundation for countries to adapt into their own national security system.