Forum: Disarmament and International Security Committee

Issue: Issue #25-02: Question on the advancement of hacktivism and the government's' vulnerability to cyber warfare

Student Officer: Woonki Park

Position: Chair of the Disarmament and International Security Committee

---

Introduction

In an age of technological advancement where access to the Internet has become a basic necessity, the compiling of data information online can be commonly seen. The United Nations has also recognized the importance of the Internet, and therefore an adjusted Article 19 of the Universal Declaration of Human Rights in November, 2016; section 32, the new extension, proclaims "The promotion, protection and enjoyment of human rights on the Internet", emphasizing the capabilities of the Internet as the modern days' means of communication, and innovation. Although the adjustment has allowed us to connect with the world, the Internet recently is being viewed as an alternative for weapons and firearms.

Cyber warfare can be described as an outcome of the Internet. Through data theft and DDos attacks across government networks, the world has reached a point where damage can be done not only physically, but in the cyber world as well. Ever since the world's first malware came into use in the 1900s, governments became more and more vulnerable to cyber attacks, leading to damage done to the victim nation's financial, military, and other branches of government network. According to BBC News, Washington D.C alone suffered from 61,000 cyber-security breaches in 2014, and more than 14 million government employees were affected by cyber attacks since 1985. In terms of economical impacts, TIME Magazine reported that "hacking costs the U.S some $300 billion per year according to some estimates. Worldwide that figure is closer to $445 billion, or a full 1 percent of global income". As a result of previous cyber attacks, researchers predict that by 2018, almost $101 billion will be spent globally on information security.

The cyber attacks that are carried out by hackers online serve many purposes, mainly for political use. Malwares that are commonly used in order to infiltrate a specific network such as viruses, trojans,

and worms are equivalent to the guns soldiers use in war zones, but instead in the cyber world. The malicious softwares allow the hacker to damage, infect, or even delete the host's data and information, completely dominating the host's network. When carrying out attacks on government networks, the hacker would most likely be using malwares to steal classified information regarding national security, temporarily shut down and bring government websites to a halt, permanently delete all of the information compiled in the network's host, and so forth. As a means to damage the victim's data network, cyber attacks may result in data theft, corruption in files, or even the loss of control over the hosted network.

Being heavily involved with ongoing conflicts taking place across the world, cyber warfare mainly involves nations with rather great political and economical power. For instance, Russia has been responsible for thousands of cyber attacks over the past years, usually targeting member states of the North Atlantic Treaty Organization (NATO). According to BBC News, the Defence Minister of Russia Sergei Shoigu admitted Russia's attacks made online, stating that "Russian 'information troops' were involved with intelligent, effective propaganda". Although exact numbers were never revealed, records show that Russian hackers carried out attacks on nations that were in conflict with Russia, as well in elections held by the United Nations' superpowers such as the United States and the United Kingdom.

Despite the impacts and casualties resulting from cyber warfare, no significant actions were so far taken in order to prevent further harm from being made. As technology advances, it is important to ensure that security advances just as much, so that both efficiency and safety remain sustainable. Currently, there are no standards settled to determine a government network's level of security, which creates a greater risk for the host from being infiltrated. To prevent cyber warfare from taking place, all member states of the United Nations should fully participate in discussions and debates in order to establish a standard on minimum cyber security in countries and develop appropriate measures to avoid cyber warfare from happening.

Definition of Key Terms

Cyber warfare

The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.

Hacktivism

The act of hacking, or breaking into a computer system, for a politically or socially motivated purpose.

Malware

Short for "malicious software", a malware is any program or file that is harmful to a computer user. Malwares include computer viruses, worms, and Trojan horses. These malicious softwares can steal, encrypt, delete sensitive data, and alter or hijack core computing functions without the owner's permission.

Virus

A type of malware designed to spread from host to host and replicate itself. It serves the purpose of altering the way how the victim computer operates by attaching itself to a document or program installed in it. When executed, a virus duplicates itself infinitely and becomes infested within the victim computer. Throughout the process password are stolen, files become corrupted, and means of communication such as email are spammed.

Trojan

A type of malware that is often mistaken to been seen as a legitimate program. Just how the Trojan Horse from Greek mythology disguised itself to look innocent and hide soldiers inside, a Trojan tricks users into installing the innocent-looking software by titling itself as an email attachment or a free program. Once activated, a Trojan enables the cyber criminal to spy on the infected computer, steal sensitive data, and even disturb computer performance.

Worm

Similar to a virus, a worm is a type of malware capable of replicating itself. What defers the two malwares is that a worm is able to spread across networks and infest not just in one computer, but all the devices that are connected to the network. Through the use of a worm, one is able to send malicious codes to other computers, delete files, and steal vulnerable information.

DDos attack

A DDos attack (distributed denial-of-service) attack is an attack in which multiple compromised

computer systems attack a target such as a server, website or other network resource in order to cause a denial of service for users of the targeted resource. It usually targets governmental networks, or major companies.

Network

A collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

Network host

A computer or other device that is connected to a computer network to communicate with other hosts on a network. A host sends and receives data stored in the network.

General Overview

As a major controversy, cyber warfare has impacted the world to a significant extent. Throughout the years of technological advancement, cases of cyber warfare affecting victim nations have also increased drastically. Listed below are some noticeable cases of cyber warfare that have contributed to this major issue.

Russia's political disruptions on the United States

Russia and the United States share a long history in terms of cyber warfare. Russia's interference on the 2016 United States elections, is simply one out of hundreds of noticeable Russian cyber attacks that have been carried out on to the US. Although many of the attacks were made in the past, the American intelligence was only able to trace Russia's footsteps recently. This year, a senior intelligence official of the United States publicly claimed that a Russian soldier had been involved in political debates online with "specifically tailored messages", and that he successfully infiltrated a U.S. social media group by pretending to be a "42-year-old American housewife". Another senior intelligence official announced that the Russian military intelligence agencies have been purchasing advertisements on Facebook in order to target specific populations in the United States with propaganda based upon Russian influences. The government of the United States continue to discover and reveal many of the cyber attacks that were carried out by Russia, however government networks are still in threat and attacks that are currently

taking place are not being discovered by the U.S. Friction between the two major powers continue to exist online, increasing the level of tension between the two nations in diverse aspects.

Russia and the United Kingdom European Union membership referendum

BREXIT, an abbreviation for "British exit", was a national referendum that took place in order to determine whether the UK wishes to remain or leave the European Union. English citizens who wished to participate in the vote had to register themselves on the English government's homepage. "GOV.UK", the government homepage that millions of English people had accessed in early June 2016 so that they could apply for their right to vote was suddenly extended to June 23. According to CNN News, the website suffered from a "DDOS attack using botnets", and displayed the message "504 Gateway Time-out" to all users of the website. The Public Administration and Constitutional Affairs Committee soon announced that "we do not believe that any such interference had any material effect on the outcome of the EU referendum", however did not deny the possibility of Russia's interference over UK's government networks. Russia did not make any comments regarding the case, however officials of the English government publicly accused Russia as the one responsible for the disruption. This is just one example of many cases where Russia brought chaos into a country's network, displaying its dominance in the cyberworld.

North Korea and its cyber attacks under Kim Jong-un

In the past decade, North Korea increased its cyber attack unit dramatically as Kim Jong-un came into power. Bureau 121, North Korea's "cyber-attack elite unit" is government-run branch of national security that specializes in cyber warfare. Due to North Korea's tendency of keeping their identities a secret, the exact location or size of Bureau 121 is unknown to the world. Recently, there have been cases of cyber attacks in which fall under the possibility of North Korea carrying out attacks on other nations. In 2014, Sony Pictures suffered from cyber attacks that were carried out to "steal movie scripts, entire films, internal memos, personal information on movie stars and Sony employees, then wipe out computers used by Sony". In February 2016, approximately $101 million was transferred from an account of the Bangladesh Central Bank to Sri Lanka and the Philippines, and the majority of the money transferred have not been fully recovered. Researches claimed that the attacks were carried out by a hacking group called "Lazarus" and that they have connections with North Korea. Because of North Korea's cyber movement being so alarming, the White House announced in 2015 that a new set of "economic sanctions" will be established to "penalize North Korea over its involvement". Not only is

North Korea becoming a threat to the real world with its nukes, but in the cyberworld as well with its hacking unit.

Hacktivists on governments

As the internet began to develop since the late 1980s, hacktivism emerged into our society as a means personal profit. However, nowadays there are millions of cases where individuals or groups of hackers independent from any governmental units carry out cyber attacks with a political purpose. A common example of hacktivism can be seen in operations executed by Anonymous, an "internal network of activist and hacktivist entities". Involved in globally significant events such as the Israeli-Palestinian conflict, the Anonymous calls for attention worldwide in order to create awareness regarding events that could create a significant impact. Through malware infestation and network shutdowns that take down the target government's servers, and public accusations on social media, hacktivists can according to sources "perhaps be the most powerful in the cyber world". Online, hacktivists could be the only group of individuals capable of opposing powerful nations and its governments. While in reality major powers such as the United States dominate the world, in the cyberworld the tables may change.

Major Parties Involved and Their Views

United States,

As one of Russia's greatest targets of cyber warfare, the United States constantly suffer from Russia's cyber attacks regarding their government. An example of this is the 2016 election, where it has been revealed that Vladimir Putin order the Russian intelligence to disrupt the election. The American intelligence reported that the hackers, who "broke into Democratic National Committee's documents" through email accounts of Democrats that were involved in the presidential race, were associated with two Russian intelligence agencies. Even though Russia denies their association with the American presidentials, the government of the US was able to reach to the conclusion that Russia had purposely made an attempt to disrupt their elections, based on Russia's previous cyber attacks. After the discovery, Barack Obama publicly warned Russia to "stay out of American elections".

China,

China has a fairly recognizable reputation in terms of cyber warfare, as it holds responsibility for

hundreds of cyber espionage cases that were discovered throughout our historical timeline. As an act of truce, President Xi Jinping visited the White House in 2015, promising not to conduct or support economic cyber espionage. Although compromises were made, China continues to spy its rivaling nations. For instance, the Chinese government was accused of hacking into the US Office of Personnel Management in early 2016, a data breach that handles data of over 21 million US citizens. The Chinese government denied their actions, however just like this China continues to infiltrate other government networks.

Russia,

The most active nation cyber-wise, Russia has been significantly gaining power online after the Cold War. Usually targeting member states of NATO, Russia is capable of placing spying softwares, stealing data from, and bringing any government network to a halt for a certain amount of time. According to Business Insider, Russia's intelligence services "decided years ago to make cyber warfare a national defense priority", and that "they have become increasingly proficient in cyber operations as a result". Russia especially has tensions risen with the United States, as they are responsible for a number of distributed denial of service (DDOS) attacks on the American government.

Iran,

Iran is becoming a "rising threat" to the global cyber warfare. Their cyber "rampage", as described by the Financial Times, began within their country when the government "unplugged" many of its cities, thus "leaving millions without electricity, crippling hospitals and military facilities". Unlike the "big five cyber superpowers - the US, UK, Israel, Russia, and China", Iran does not focus on a specific target, it "just wants to do as much damage as possible". Accompanied by its cyber campaign "Abadil campaign" which involves "crude, low-tech denial of service attacks to overwhelm websites, combined with acts of digital vandalism", Iran is emerging as the sixth cyber superpower.

Israel,

The Israeli Defense Forces (IDF) uses hacking as their main tool for dealing harm to its enemy countries. As a cyber superpower, Israel possesses fairly advanced skills used in cyber warfare. One of Israel's biggest achievements, according to Israel National News, is the code in which IDF uses in cyber warfare, as no country was ever able to decode Israel's codes. Due to their codes being unrecognizable, foreign hackers are left helpless once they hack into Israeli military networks, since it is impossible to

decode and create new lines of code to their advantage, This gives Israel a huge advantage once in conflict with other nations.

North Korea,

North Korea possess a national cyber warfare agency called "Bureau 121". Due to its well-structured security, foreign hackers are unable to determine its exact size, however it is assumed that operations are performed from outside the country. It has been discovered that North Korea's educational system promotes computing, and the best students are then chosen and trained by the military to become national hackers serving for Bureau 121. The cyber warfare agency targets South Korea, and holds responsible for most of data breaches taking place in South Korea.

South Korea,

Although it is noticeable for its fastest Internet speed in the world, South Korea rarely performs cyber attacks on other countries. Instead, South Korea is the biggest victim of cyber attacks carried out by North Korea and Bureau 121. According to CNN News, more than 140,000 computers and 160 security firms were hacked by North Korea as of June 2016. The fact that the entire country is technologically advanced allows its citizens to be more vulnerable to cyber attacks in comparison to other countries. The government trains its own "cyber army" in order to oppose North Korea's Bureau 121, however it only accepts 30 students a year and is uncomparable to North Korea's "cyber army".

NATO,

Member states of the North Atlantic Treaty Organization are the main targets of cyber attacks carried out by Russia. The NATO Review Magazine reported that two main types of cyber attacks in which NATO member states are in particular vulnerable to are cyber espionage and cyber sabotage. As a means of protection, NATO currently prioritizes security against threats existing in the cyberspace, and assists its member states in "developing their own cyber defence capabilities and capacity".

Timeline of Events

1988	The Morris worm, one of the "first recognised worms to affect the world's nascent cyber infrastructure" was spread in the U.S. The malware decreased its

	hosting computer's speed processor speed till the point where the computer became unusable.
December 2006	NASA forced to disallow its employees from opening emails with attachments as a means of preventing data theft.
April 2007	Estonian government networks were shut down due to a series of DDos attacks. "some government online services were temporarily disrupted and online banking was halted."
June 2007	An unclassified email account owned by the US Secretary of Defense was hacked by unidentified intruders as part of a larger series of attacks, disrupting the Pentagon's network.
October 2007	The Chinese Ministry of State Security claimed that foreign hackers, 42% from Taiwan and 25% from the United States, had been stealing information from "Chinese key areas".
Summer 2008	The databases of Republican and Democratic campaigns were accessed without permission and downloaded by unknown intruders.
January 2009	Israel's main internet infrastructure was attacked during the Gaza War. Government websites were the main targets of the attack, which resulted in at least 5,000,000 computers temporarily executed. The Israeli government soon announced that the attack was carried out by a "criminal organisation based in a former Soviet state, and paid for by Hamas or Hezbollah.
January 2010	A group of hackers from Iran named the "Iranian Cyber Army" disrupted China's popular search engine "Baidu". The attack disallowed users from accessing the website, and instead redirected them to a page showing an Iranian political message.

October 2010	Stuxnet, a type of malware designed to be infested within the industrial control systems of "Siemens", a German electronics company, was discovered in Iran and Indonesia. The discovery led to the assumption that the malware was a "government cyber weapon aimed at the Iranian nuclear programme".
January 2011	The government of Canada claimed that its agencies including Defence Research and Development Canada (a research for Canada's Department of National Defence) were suffering from cyber attacks. The series of cyber attacks forced the Finance Department and Treasury Board to disconnect from the Internet.
October 2012	Kaspersky, a Russian cyber security company discovered a "worldwide cyber-attack dubbed 'Red October'". Hackers who were responsible of the attacks spied on Microsoft Word and Excel documents in order to gather information of its users. Targets of the attack usually appeared in Europe, North America and Central Asia, involving government embassies, research firms, military installations, nuclear and other "critical infrastructures".
March 2013	South Korea's financial institutions and their national broadcaster YTN had their networks affected by cyber attacks carried out by North Korea.

UN involvement, Relevant Resolutions, Treaties and Events

So far, the United Nations has hardly made any actions in order to address this ongoing issue. Although cyber warfare has developed into a global issue, the United Nations does not have its official definition of the term, which may demonstrate the United Nations' lack of concern regarding cyber warfare. The only ways in which the United Nations has been involved are limited to resolutions passed as a means to provide its member states with meaningful guidelines regarding cyber security and warfare. Many member states of the United Nations beyond the P5 are capable of conducting cyber attacks, and at the same time threatened by the possible scenario of becoming victims of cyber warfare. As the issue has never been formally addressed by the United Nations, actions need to be taken by the intergovernmental organization so that the issue does not increase in scale and damage.

- Creation of a global culture of cybersecurity, 31 January 2003 (**A/57/529/Add.3)**
- Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 30 January 2004 **(A/58/481/Add.2)**

Evaluation of Previous Attempts to Resolve the Issue

There were not many noticeable attempts made to resolve the issue, but one noticeable event that created a significant impact regarding cyber warfare was the Council of Europe's Budapest Convention on Cybercrime which took place in 2001. The convention, which involved European cyber powers such as Russia, addressed growing concerns over cyber security throughout Europe. All member states of the Council of Europe were obliged to sign the treaty and agree to all of the articles regarding cyber attacks, security and warfare that were passed by the Council. The treaty came into effect in 2004 and limited cyber attacks carried out by governments on other nations within the European continent, thus promoting privacy and safety in the cyber world.

Possible Solutions

One of the main factors that contribute to the development of cyber warfare is the great lack of the United Nations' involvement in the issue. The United Nations, an international organization consisting of countries worldwide was formed in order to maintain order and peace in our society. The committee that mostly deals with issues that threaten one's safety is the Security Council, which was established in order to provide the world with resolutions that could prevent the issue from creating more harm. Ever since the establishment of the United Nations, the Security Council played a key role of dispatching peacekeeper troops in regions of warfare.

The committee has always been responsible for discouraging enemies from conflict and ceasing wars, however the Security Council has never been involved in conflict that took place away from war zones. Cyber warfare is undeniably an ongoing war that threatens many of the United Nations' member states, but there are no peacekeepers that are capable of combat in the cyber world. A branch of United Nations peacekeepers that specializes in hacking and carrying out cyber attacks against threatening hacktivist groups could be a solution to prevent the loss of government resources such as classified military information or financial data. Just as how in real warzones the United Nations peacekeepers are able to cease conflicts through military dominance, a powerful cyber warfare unit that is able to maintain

order in the cyber world could be a solution to this issue.

Bibliography

Hern, Alex. "Cyber-attacks and Hacking: What You Need to Know." The Guardian. Guardian News and Media, 01 Nov. 2016. Web. 03 June 2017. <https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime>.

Denning, Dorothy. "The Rise of Hacktivism."Georgetown Journal of International Affairs. N.p., 8 Sept. 2015. Web. 03 June 2017. <http://journal.georgetown.edu/the-rise-of-hacktivism/>.

Lohrmann, Dan. "Understanding New Hacktivism: Where Next for Hackers With a Cause?" Government Technology: State & Local Government News Articles. N.p., 31 July 2016. Web. 03 June 2017. <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/understanding-new-hacktivism-where-next-for-hackers-with-a-cause.html>.

Stout, Kristie Lu. "Cyber Warfare: Who Is China Hacking Now?" CNN. Cable News Network, 29 Sept. 2016. Web. 03 June 2017. <http://edition.cnn.com/2016/09/29/asia/china-cyber-spies-hacking/>.

Robinson, Neli. "NATO: Changing Gear on Cyber Defence." NATO Review. N.p., n.d. Web. 03 June 2017. <http://www.nato.int/docu/Review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm>.

Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times. The New York Times, 13 Dec. 2016. Web. 03 June

2017.

<https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html>.

Beaver, Michael. "The United Nations and Cyberwarfare." Global Risk Advisors. N.p., 10 Apr. 2017. Web. 03 June 2017. <https://globalriskadvisors.com/blog/united-nations-cyber-warfare/>.

Lee, Dave. "Bureau 121: How Good Are Kim Jong-un's Elite Hackers?" BBC News. BBC, 29 May 2015. Web. 04 June 2017. <http://www.bbc.com/news/technology-32925503>.

Harley, Brian. "A Global Convention on Cybercrime?" Columbia Science and Technology Law Review. N.p., 23 Mar. 2010. Web. 04 June 2017. <http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/>.

Appendix or Appendices

Please include any materials that you may wish to Appendix in this section. Also, Roman numerals must be used in labeling the different appendices. It is highly recommended that any useful links be placed in this section.

- Cyber-attack overview:

  https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime

- Cyberwar superpowers:

  https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

- Timeline of cyber attack cases:

  http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

- United Nations' resolution on cybersecurity:

  https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

- A Global Convention on Cybercrime:

http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/