



Committee: Legal Committee (GA 5)
Issue: Defining the legality of cyber attacks
Student Officer: Alp Kelimet (President Chair)

Introduction to the Issue

“I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones.”

-Albert Einstein

Cyber Warfare could be used in World War III if we don't take action. In the era of advanced warfare, with the developing technology, the wars are changing from human-based to cyber-based battles. A cyberattack is the exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks are mostly implemented by individuals, however, some cyber-attacks can be government assisted. Cyber attacks can be performed for multiple occasions. Most common ones are identity theft, fraud, malware, spamming, Trojans and viruses. Also there are some types of cyber attacks that violate the right to privacy such as password sniffing, private and public web browser exploits Intellectual Property (IP) theft or unauthorized access. The issue about the legality of cyber attacks is that every country has their own laws against cyber attacks therefore there is no international definition of cyber attacks.

Involved Countries & Organizations

People's Republic of China

People's Republic of China has been involved in cyber attacks more than other countries. China involved in major cyber attacks such as 2009 Google attack and 2015 GitHub attack. Most Chinese cyber attacks aimed US industry however, in 2015 they reached an agreement. The cyber attacks have decreased after the agreements.

Anonymous

Anonymous is a hactivist organisation which was established in 2008. They conducted many DDoS and other cyber attacks aiming governmental bodies. Anonymous is the biggest and the most famous hactivist organisation. Anonymous' members are unknown. They release videos to threaten



governments. For example, Anonymous released a video after Paris terrorist attack in 2015, to accuse Turkish Government with helping ISIS and threaten.

Russian Federation

Despite the fact that Russian Federation has been involved in many cyber attacks, it also faced cyber attacks. According to President Vladimir Putin, Russia received more than 25 million cyber attacks during World Cup 2018. Russian Federation was involved in 2016 United States Presidential Election by leaking Hillary Clinton's emails which led to some strong accusations.

United States of America

United States of America has one of the strongest cyber warfare. Although United States' cyber warfare is strong, it faced huge cyber attacks including the one concerning presidential elections. US suffered various cyber attacks including 2000 MafiaBoy attack, 2009 Google attack from China and 2015 GitHub attack. In 2016 Hillary Clinton's emails were leaked to damage her election campaign. Strong accusations were made to Donald Trump for collaborating with Russia to damage Clinton's campaign.

North Atlantic Treaty Organisation (NATO)

North Atlantic Treaty Organisation has a sub-branch upon cyber security. NATO is aiming to improve its cyber defense. NATO and European Union are cooperating upon strengthening relations for cyber defense.

Detailed Analysis of the Issue

According to the 12th article of Universal Declaration of Human Rights, everybody has the right to have privacy, The Article states that no one is constrained to interference with their privacy. Although the right to privacy is protected under the most important resolution about human rights, major violations has been made by numerous countries and powerful organizations. In 2018 World Cup, approximately 25 million cyber attacks were neutralized according to President Vladimir Putin. Also in the same year, Facebook's Chief Executive Officer Mark Zuckerberg faced a trial in Washington, USA for violating user agreement and taking advantage of the data of millions of users.



Types of Cyber Attacks

The most common type of cyber attack is distributed denial-of-service, also known as, DDoS attacks. DDoS attacks are basically an attack on system which makes the system occupied and not available for service requests. 2016 Dyn, major DNS (Domain Name System) provider, was under a DDoS attacks which caused the interruption of famous sites as Netflix, PayPal, The New York Times and Reddit. Also in 2015 World's leading software development platform, GitHub was under DDoS attack which was the World's biggest DDoS attack. The importance of this attack was the DDoS traffic originated China and created strong allegations against People's Republic of China. The other common type of cyber attack is the man-in-the-middle (MitM) attack. A MitM attack occurs when a hacker inserts itself between the communications of a client and a server such as Session Hijacking. Malware attacks are the third type of cyber attacks. Malware attack can be described as an unwanted software in the system that is installed without your consent. The most common type of Malware is Trojan. Trojan is a program that hides in a useful program and usually has a malicious function. Trojan Malware is named after Trojan Horse. The cyber attacks continue with Drive-by attacks, Password attacks and Birthday attacks.

United Nations Universal Declaration of Human Rights

United Nations Universal Declaration of Human Rights is one of the milestone documents in the history of Human Rights. It was drafted by various representatives from different cultures. It was adopted by United Nations General Assembly on 10th December 1948, Paris. Universal Declaration of Human Rights has 30 articles which aimed to look after the basic rights and needs for every single human being.

Article 12

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

The 12th Article of Universal Declaration of Human Rights assures the right of privacy. The interference which is stated in the Article covers physical violation of privacy however, Intellectual Property (IP) theft can be considered as a violation of privacy in 21st century.

2016 United States Presidential Elections

The United States' Presidential Elections is one of the most discussed Presidential Elections in the history of USA. Republican Candidate Donald J. Trump was elected as President against Democrat



Hillary Clinton. Before the elections Hillary Clinton's emails were leaked in WikiLeaks. Hillary Clinton stated that she made a mistake by using personal email account from her private property in New York. Federal Bureau of Investigation started an investigation. But this was not the only suspicious issue with the 2016 Elections. Strong allegations were stated against President Vladimir Putin and Kremlin Government for interfering with US elections and helping Donald Trump. According to US intelligence agencies hackers from Russian Federation used a similar technique to Trojan Malware. The allegations became stronger on 27th February 2018 when President Donald Trump's former lawyer Michael Cohen testified in the Congress, stating Mr Trump's relevance with Russia in elections, how he is a liar and racist.

List of Important Events

10 December 1948	Universal Declaration of Human Rights was adopted by General Assembly that secured the right to privacy.
2000	15 year old high school student Michael "MafiaBoy" Calce distributed DDoS attacks on famous sites as Yahoo, Amazon and eBay damaging 1.2 billion \$.
2003	Hactivist organisation Anonymous was established.
2009	World's most used search engine, Google, was under a cyber attack from China.
April 2011	Sony PlayStation Network was attacked, personal data of 77 million users were leaked.
January 2014	100 million credit cards were stolen and 20 million bank accounts were hacked in South Korea. Employee of Korea Credit Bureau was behind the theft.
August 2014	IT security company Hold Security revealed that Russian hackers stole 1.2 billion login and passwords on 420.000 websites.
2015	GitHub was under a DDoS attack from China.



2016	Netflix, PayPal, The New York Times and Reddit was interrupted because of a DDoS attack to Dyn.
2016	Hillary Clinton's email leaked to WikiLeaks to damage Clinton's Election campaign.
2016	Hackers from Russian Federation tried to hack United States Governmental Branches including White House using bait emails.
10 April 2018	Facebook's Chief Executive Officer Mark Zuckerberg testified in court for selling private information and violating user agreement.
June 2018	Vladimir Putin stated Russian Federation faced more than 25 million cyber attacks during World Cup 2018.
27 February 2019	Donald Trump's former lawyer Michael Cohen testified in Congress, accusing that Mr. Trump agreed with Russia for leaking Clinton's emails and damaging her campaign.

Past Resolutions and Important Documents

- Creation of a global culture of cybersecurity and protection of critical information March 2010 (Resolution 64/211)
[A/RES/64/211](#)
- Creation of a global culture of cybersecurity and the protection of critical information infrastructures, January 2004, (Resolution 58/199)
[docs/UN_resolution_58_199.pdf](#)
- Creation of a global culture of cybersecurity January 2003 (Resolution 57/239)
[docs/UN_resolution_57_239.pdf](#)



- Combating the criminal misuse of information technologies January 2002, (Resolution 56/121)
[docs/UN_resolution_56_121.pdf](#)
- United Nations Universal Declaration of Human Rights, 10 December 1948 (GA Resolution 217A)
[A/RES/217\(III\)](#)
- Combating the criminal misuse of information technologies January 2001, (Resolution 55/63)
[docs/UN_resolution_55_63.pdf](#)
- Council of Europe Treaty no.108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 28 January 1981
[documentId=0900001680078b37](#)

The Universal of Declaration Human Rights granted the right to privacy with 12th article. Resolutions numbered 57/239, 58/199 and 64/211 were aimed to create global culture of cybersecurity however, they are not efficient since countries failed to establish cooperation on this issue. Resolutions 56/121 and 55/63 were aimed to combat the criminal misuse of information technologies by explaining the juristical consequences of cyber crimes. The resolution were not efficient due to Government assisted cyber attacks as 2015 GitHub China assisted cyber attack or 2018 World Cup cyber attacks.

Past Attempts to Solve the Issue

United Nations tried to create international definition of cyber attacks, but it failed when countries failed to establish cooperation. Also United Nations tried to make an international definition of cyber attacks, which is also failed due to unsuccessful cooperation. United Nations' attempts have failed however, North Atlantic Treaty Organisation has an efficient attempt. NATO established a sub-branch to protect its allies against cyber attacks.



Possible Solutions

Establishing cooperation between countries will be efficient. For example, an agreement between United States and China were made and cyber attacks decreased. A convention will be efficient between the countries such as United States, Russia, China and North Korea since they are the most involved countries in cyber attacks. Another possible solution is the defining the consequence of cyber attacks internationally. Finding an international definition of cyber attacks will promote the issue. Also establishing a sub-branch of United Nations against cyber attacks will unite the countries. For example North Atlantic Treaty Organisation has a sub-branch upon cyber security which aimed to protect its allies.

Bibliography

“Cyber Attack - What Are Common Cyberthreats?” *Cisco*, 25 Feb. 2019,
www.cisco.com/c/en/us/products/security/common-cyberattacks.html

“What Is a Cyberattack? - Definition from Techopedia.” *Techopedia.com*,
www.techopedia.com/definition/24748/cyberattack

“Top 10 Most Notorious Cyber Attacks in History.” *ARN*, 27 Feb. 2019,
www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

“Top 10 Most Common Types of Cyber Attacks.” *Netwrix Blog Introduction to Active Directory Services Technologies Comments*,
blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

Harding, Luke. “What We Know about Russia's Interference in the US Election.” *The Guardian*, Guardian News and Media, 16 Dec. 2016, www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election

Zurcher, Anthony. “Hillary Clinton Emails - What's It All about?” *BBC News*, BBC, 6 Nov. 2016,
www.bbc.com/news/world-us-canada-31806907



Nato. "Cyber Defence." *NATO*,
www.nato.int/cps/en/natohq/topics_78170.htm

Statistics,
www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

"Live Cyber Attack Threat Map." *Live Cyber Attack Threat Map* | *Check Point Software*,
threatmap.checkpoint.com/ThreatPortal/livemap.html