Forum: General Assembly 6

Issue: Effective measures to address cybercrime in all its forms

Student Officer: Amina Hedider

Position: Deputy Chair

Introduction

The first cybercrime recorded took place in 1820. The first major wave in the late 80's. It is now 2018 and cybercrime is still an ongoing issue in our world. Cybercrime is currently the fastest growing area of crime worldwide, due to the fact that it is seen as an easy way to make a profit with little to no risks and, if caught, punishments also are perceived as low. This international form of crime is causing serious harm and imposing threats to victims worldwide. The speed and anonymity of the internet are being exploited by criminals. There are currently many complex cybercriminal networks around the globe that unite individuals together in order to commit these crimes. Criminals have been using the internet to facilitate their actions and maximize profit in a shorter period of time. These crimes include theft, fraud, illegal gambling and the sale of fake medicine, all of which can cause harm to society. There are two main types of cybercrime, advanced cybercrime and cyber-enabled crime. Advanced cybercrimes are attacks against computer software and hardware, whereas cyber-enabled crimes are more traditional types of crimes such as terrorism. Both, almost equally as bad.

It is vital to take notice of the increasing numbers of internet users as 55% of the world's population have access to the internet, allowing cybercriminals to have countless targets and endangering more people. Cybercrime is a difficult issue for reasons such as the constant advances in technology, the difficulty of gathering evidence, and the fact that it is transnational. Cybercrime is a transnational form of crime and therefore, it is vital for countries to work together. Cybercrime can be committed anywhere around the world so a country cannot eradicate cybercrime in its borders by itself, it needs assistance in order to catch the criminals committing these crimes.

Definition of Key Terms

Cybercrime

It is an illegal criminal activity carried out by a computer or other devices connected to a network. Examples of cybercrimes include: Fraud, identity theft and hacking.

Advanced Cybercrime

Advanced cybercrime is attacks against computer software and hardware, It is an attack by hackers, they could be organisations or individuals. They infiltrate devices without a right and can cause both direct and indirect damage, theft and harvesting.

Cyber Enabled crime

Cyber-enabled crime is committing “traditional” crimes such as financial crimes and crimes against children and terrorism through the internet. They are crimes that could be committed without the internet but the use of the internet makes these crimes easier and less risky to commit.

Cybersecurity

The techniques or strategies of protecting devices from hackers, viruses or any other sort of unauthorized access to the device.

Phishing

Phishing is a type of fraud. It is attempt at stealing personal or private information such as usernames passwords, phone number or credit card number.

Pharming

Pharming is redirecting users to different sites. An example of this is used in illegal websites when watching movies.

Background Information

Previously, cyber crime was committed by mainly small groups or individuals. However, now there are highly complex cyber criminal networks that get individuals together in order to commit crimes, and this is even more dangerous. It is vital for member nations to work together in order to ensure that the internet remains safe for everyone to use it and that the sharing of all information is dealt with in an appropriate manner. One of the main reasons that countries must work together is that cybercrime can be committed anywhere across the globe so a country by itself cannot eradicate cybercrime in its borders by itself, it needs assistance in order to catch the criminals committing these transnational crimes. The main reason that makes cybercrime a common act is that its very profitable and it includes very little to

no risks. One of the reasons it is very profitable is that sensitive data such as data owned by major sectors of countries such as military can be manipulated to cause major damage to a nation.

Types of Cybercrime

There are two main types of cybercrime, advanced cybercrime and cyber-enabled crime. Advanced cyber crime is used in attacks against the computer software and hardware. Advanced cybercrime is the attack by either hackers, individual or groups. They infiltrate devices without a right and can cause either direct on indirect damage these could include harvesting or theft. On the other hand, cyber-enabled crime are more traditional types of crimes such as terrorism or crimes against children using the internet.

Identity Theft

This is example of a form of cybercrime is extremely easy to commit because it attacks individuals directly and on a personal level. Identity theft is the stealing someone's identity, their name and information to gain financial advantage or get benefits under the other person's name. In addition to that, the amount of money that is being stolen by individuals has risen dramatically, these sorts of attacks can lead to the victims having huge financial losses and ruin their reputation on credit reports for example.

Hacking

Hacking is finding weaknesses to gain unauthorised access to a network or a computer to exploit it's weaknesses. Hackers can change things such as security features. Hackers employ various techniques such as password cracking. Hackers can cause damage to computers and other devices as well as humans in ways such as losing of information, hacking often results in a loss of data as files can be stolen or deleted. In addition to information loss, financial losses can also take place. When a computer or device is hacked the hackers gain access to your computer, this decreases people's privacy as well.

Phishing

Phishing is an attempt to access sensitive information such as passwords, usernames, banking and credit card details. Targets are usually contacted through telephone, email, or text message by posing as legitimate institutions to trick people into providing sensitive data or into opening an email, the recipient is then lured into clicking on a link which can then lead to the installation of malware or revealing sensitive information. There are two types of phishing, email scams and spear phishing. Spear phishing targets a specific organisation as opposed to random people like email scams. The act of phishing harms people. For individuals, it can result in identity

theft or unauthorized purchase and for companies, this may lead to severe financial losses as well as a decrease in market share and consumer trust.

Major Countries and Organizations Involved

International Police Organisation (INTERPOL)

The International Police Organisation has a huge role in the issue of cybercrime. INTERPOL is an organisation that is committed to fighting cybercrime and cyber-enabled crimes, Their main initiatives include operational and investigated support, cyber intelligence and analysis and many more. This organisation tries to advance the fight against cybercrime through proactive research into emerging crimes and latest training techniques and the development of new innovative policing tools. They have and continue to play a crucial part in tackling cybercrime. In 2014 INTERPOL has opened the IGCI (interpol global complex for innovation), a research facility to find more effective ways to tackle this issue. This organisation has also implemented a two year project to help countries in latin america and the caribbean to combat cybercrime. Furthermore, INTERPOL also carries out a variety of activities to support its member countries to fight cybercrime, activities that interpol carry out include- providing support in cybercrime investigations; working to develop new technology; conducting training sessions and assisting nations in reviewing their cyberfight capacities. In addition to this, the organization hosts the Europol cybercrime conference. This conference brings together experts from around the world to further strengthen international networks to combat these sorts of crimes.

United States of America

The US is one of the biggest victims of cybercrime in the world, it has the highest rate of cybercrime . The United States has implemented numerous programs such as a federal agency called national institute of standards and technology (NIST) to ensure cyber security is at its strongest possible, NIST developed a cybersecurity framework that addresses cyber threats and supports businesses or organisations by managing their cybersecurity risks, this framework also helps them respond to and recover from cybersecurity incidents. It also hosts a yearly cybercrime conference that promotes training and support to agencies on how to tackle causes where technology is the weapon to commit crimes. In addition to this, the Department of Homeland Security (DHS) is also deeply concerned and is making an effort to combat cybercrime. DHS works with numeral federal agencies to conduct efficient and effective criminal investigations to combat cyber criminals and prioritize the training and recruitment of technical experts. DHS also has a special division dedicated to combat cybercrime. Over the years, the US has also been working with China to try and improve counter measures against cybercrime.

China

China has the 2nd highest rate of cybercrime in the world. Citizens of china are victims of crimes such as fraud and stolen identity. Despite the high amount of cybercrime incident, China has not signed any treaties with the European Union or any other nation on data protection. A reason for high rates of cybercrime in China could be because there are short prison sentences for those convicted and these sentences are getting even shorter. China also has recently taken steps to develop its data protection laws, such as the cybersecurity law that came into effect in 2017 and regulatory measures are being issued regularly to supplement its provision. China has also issued a couple of internet rules that prohibit anyone to propagate viruses and scams. In 2014, they released a policy paper where it showed its willingness to cooperate with the EU on the issue of cybercrime and start strategizing plans to abolish it.

Russian federation

The Russian Federation is known to reject international cooperation to solve cybercrime with foreign law enforcement. Russia is not part of the 55 parties that have signed to follow and implement the Budapest Convention of Cybercrime in their national legislation, they rejected it due to the lack of overlap between the conventions ideas and the Russian policies, in addition to this, Russia also opposed the practice ever since the US police hacked computers belonging to two Russian men and discovered that they had been defrauding American banks. However, Russia was part of the G8 that made an effort to combat cybercrime. The G8 all agreed to a plan to tackle international cybercrime, the agreements main aims were to fight cyber crimes such as drug-trafficking, money-laundering, paedophilia, electronic fraud and espionage. Later on, Russia was suspended from the G8 as it had invaded and annexed Crimea (Ukraine) illegally. In Russia, state sponsorship of cybercriminals is a major issue, furthermore, Russia has been suspected of supporting various attacks in Ukraine, all of which were designed to weaken support for the leaders and present its public services as ineffective.

UNODC

Over the years, UNODC has promoted sustainable and long term help and solutions to the fight against cybercrime in many way such as supporting national structures and actions. The UNODC refers to its justice system to provide technical assistance in prevention and awareness raising, data collection and the research and analysis on cybercrime. In 2017, UNODC started the cybercrime program, the key aims of this program were to increase the efficiency and effectiveness in investigations and adjudication of cybercrime. Another aim was to get effective long term government responses to cybercrime and to strengthen communication between governments. Additionally, in 2015 the UNODC, under the framework of the Commission on Crime Prevention and Criminal Justice, launched a cybercrime

repository. This aims to assist countries in to prevent cybercrime and to effectively prosecute cybercriminals.

Timeline of Events

Date	Description of event
1986	Congress passes computer fraud and abuse act, making hacking and theft illegal.
1994	Launch of the World Wide Web.
1997	The G8 have a meeting in Washington D.C to start a foundation against cybercrime.
1998	The first major attack occurred on a government website.
2001	The Budapest convention is drafted and ratified by the council of Europe.
2003	The additional protocol is added to the Budapest Convention.
2004	The Europe convention of cybercrime came into effect.
2013	The European cybercrime centre starts working.
2014	China shows its willingness to cooperate with the EU on the issue of cybercrime.
2015	UNODC under the framework of the Commission on Crime Prevention and Criminal Justice launched a cybercrime repository.
2016	Cybercrime scandal where it was thought the american presidential election was hacked by Russia.
2017	UNODC started their cybercrime combatting program.

Relevant UN Treaties and Events

- The Budapest Convention of Cybercrime, 1 July 2004
- Prevention, protection and international cooperation against the use of new information technologies to abuse or exploit children, 28 July 2011 **(E/RES/2011/30)**
- Twelfth United Nation Congress on Crime Prevention and Criminal Justice, 1 April 2011 **(A/RES/65/230)**
- Conducting a comprehensive study of the problem of cybercrime, December 2010 **(A/RES/65/230)**

- Strengthening the United Nations crime prevention and criminal justice programme, 27 March 2013, **(A/RES/67/189)**
- United Nations Convention Against Transnational Organized Crime **(Resolution 55/25)**
- Strengthening international cooperation to combat cybercrime, 2013 **(Resolution 22/7)**
- Comprehensive Study on Cybercrime, **February 2013**
- Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime, 2013 **(Resolution 22/8)**
- Crime Prevention **(Resolution 22/7)**

Previous Attempts to solve the Issue

The formation of the G8 group can be considered one of the first multinational attempts to solve this issue.The G8 group consisted of France, Germany, Italy, United Kingdom, Japan, the United States, Canada, and Russia. They decided to get together to focus on combating the many different types of cybercrime. The most important measure established was the training of local law enforcement officers to deal with cybercrimes. There was a 24/7 hotline service for cybercrime reports and complaints; this would help the police respond to cyber attacks more quickly and provide advice on how to catch criminals in a concise manner. However, the G8 planned to get other nations involved but failed. This was mainly due to LEDCs being unwilling to meet the demands and standards set up by the G8, which include: Contact point available 24/7, contact point must have basic english lang, contact point must have basic technical skills, contact point must be familiar with domestic laws and policies.

A key attempt to solve this issue was the Budapest Convention. It provided the world a great first step to fight against cybercrime.The Budapest convention is also known as the convention on cybercrime. Its one of the only guidelines introduced by the council of europe and one of the only binding international instrument on the issue of cybercrime. It is a foundation for legislation for which countries agreed on and the amount of members continues to grow. It is a framework used to enhance international cooperation of member states. It also covers the fundamentals to working against cybercrime. The treaty is something that governments could potentially use to help model their policies against cybercrime. It also concludes procedure that law enforcement could integrate into laws to help capture cybercriminals. However, As a result of the guideline being drafted by the European Council, non-EU countries such as India ratified as it wasn't involved in the drafting process. This failed because countries who just refused to ratify like Russia hindered the guideline of its full potential.

In 2014, interpol opened the Interpol Global Complex for Innovation in Singapore (IGCI). The IGCI is a research and development facility. It leverages global cyber expertise from law enforcement. There were also regular engagement at the working group meetings on cybercrime for heads of units

stakeholders from across Americas to get together and try to discover more effective strategies to combat cyber threats, this helped countries that needed additional help or support in developing their cyberinfrastructure. This was successful due to effective working relations with the countries, national law enforcement, judicial agencies, and international organisations.

An ongoing attempt to solve this issue is the Europol cybercrime conference, also held by interpol. The first ever conference took place 2013, it alternates every year between Europol's European Cybercrime Center in The Hague and the INTERPOL global complex for innovation in Singapore. The main aim of these conferences is to bring together experts from cybercrime divisions worldwide to further strengthen international networks against cybercrime.

Furthermore, NIST promotes awareness of their cybersecurity framework, this framework addresses cyberthreats and supports organisations and businesses by managing their cybersecurity framework and helps them respond to and recover from cybersecurity incidents. This however, only helps organationisations that understand their cyber security risks, threats, vulnerability and impact.

Possible Solutions

It is necessary to make all nations aware of the risks, threats, impact and severity of cybercrime has on our world. This could be bone through international workshops with experts from organisations such as INTERPOL or UNODC, where all member states are invited to participate. This will help lead to a global understanding of this issue and ensure that citizens and their data are safe. Citizens have one of the main roles when is comes to the development of countries therefore, the UN encourage the regulation of digital networks to ensure that people have the right access to information they need in a legal manner. INTERPOL has already designed an international body to combat cyber crime but some countries do not cooperate with them due to the lack of overlap with the country's policies, therefore the UN can try to tailor INTERPOL’s policies around countries policies in order to increase overlap. This makes moving forward to tackle this issue difficult because since cybercrime is a transnational form of crime, all countries must work together as it can be committed anywhere across the globe and therefore a country, cannot eliminate cybercrime in its borders by itself, it needs help in order to catch the criminals.

A possible way to combat cyber crime internationally would be getting INTERPOL to train national law enforcement with basic training in dealing with cybercrime. INTERPOL would implement this because it will help reduce cybercrime on an international level which is their goal. In cases where the cybercrime is transnational, INTERPOL would be the ideal agency to oversee the peaceful collaboration between the countries. A major setback is that some nations do not have the capabilities to make cybercrime a high priority issue on the government’s agenda as they have other, more pressing issues

they have to deal with. Therefore, the UN would become able to aid these countries in being able to address cybercrime domestically and internationally.

The internet has penetrated almost every aspect of people's day to day lives and this has opened criminals more opportunities to target new victims. Therefore, people protecting themselves from these criminals is vital. As the criminals are always looking for ways to manipulate, updating safety measures regularly is crucial to remain safe from cyber criminals at all times. The UN could increase awareness on how to stay safe and encourage the people to use antivirus softwares such as firewall or anti-spyware tools as well as being alert to phishing scams; only connect to wireless networks that are encrypted and not to open emails, links or other attachments sent by people you don't trust or any untrusted sources. Passwords should be unique and complex to prevent people from gaining access to your private accounts, this could be done by including a variety or symbols, caps and lowercase letters.

Bibliography

"Cybercrime." *Cybercrime / Cybercrime / Crime Areas / Internet / Home - INTERPOL*, www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

"Online Safety." *Online Safety / Cybercrime / Crime Areas / Internet / Home - INTERPOL*, www.interpol.int/Crime-areas/Cybercrime/Online-safety.

"Overview." *United Nations*, United Nations, www.un.org/en/sections/about-un/overview/index.html

"Cybercrime." *Cybercrime / Cybercrime / Crime Areas / Internet / Home - INTERPOL*, www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

akara.umapornsakula. "United Nations Office on Drugs and Crime." *Cybercrime*, www.unodc.org/southeastasiaandpacific/en/what-we-do/toc/cyber-crime.html.

"Online Safety." *Online Safety / Cybercrime / Crime Areas / Internet / Home - INTERPOL*, www.interpol.int/Crime-areas/Cybercrime/Online-safety.

agustina.diaz-rhein. "United Nations Office on Drugs and Crime." *Index*, www.unodc.org/unodc/en/cybercrime/index.html.

"Cybercrime." *Cybercrime / Cybercrime / Crime Areas / Internet / Home - INTERPOL*, www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

"Cybercrime: Understanding and Addressing the Concerns of Stakeholders." *Computers & Security*, Elsevier Advanced Technology, 21 July 2011, www.sciencedirect.com/science/article/pii/S016740481100085X.

11, 2017 Jan. "5 Strategies for Addressing Cybercrime." *GCN*, gcn.com/Articles/2017/01/11/strategies-addressing-cybercrime.aspx?Page=2

Google Search, Google, www.google.com/search?q=resons%2Bfor%2Bcybercrime&rlz=1C5CHFA_enQA696QA696&oq=resons%2Bfor%2Bcybercrime%2B&aqs=chrome..69i57j0l2.5693j1j7&sourceid=chrome&ie=UTF-8.

Nohe, Patrick. "2018 Cybercrime Statistics: A Closer Look at the 'Web of Profit.'" *Hashed Out by The SSL Store™*, 27 Sept. 2018, www.thesslstore.com/blog/2018-cybercrime-statistics/.

Dennis, Michael Aaron. "Cybercrime." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 9 Mar. 2018, www.britannica.com/topic/cybercrime.

Ray, Sanjana. "4 Types of Cybercrime That Everyone Should Know About." *YourStory.com*, Yourstory, 2 Dec. 2016, yourstory.com/2016/12/4-types-of-cybercrime/

UNODC study on cybercrime https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Full List." *Treaty Office*, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Brown, Justine. "5 Federal Agencies with a Role in Ensuring Enterprise Cybersecurity." *CIO Dive*, 17 Aug. 2016, www.ciodive.com/news/5-federal-agencies-with-a-role-in-ensuring-enterprise-cybersecurity/424557/.

agustina.diaz-rhein. "United Nations Office on Drugs and Crime." *Index*, www.unodc.org/unodc/en/cybercrime/index.html.

"INTERPOL Cybercrime Capacity Building Project in Latin America and the Caribbean." *Regional Approach / INTERPOL Cybercrime Capacity Building Project in Latin America and the Caribbean / Cyber Americas / Multi-Year Programmes / INTERPOL Expertise / Internet / Home - INTERPOL*, www.interpol.int/INTERPOL-expertise/Multi-year-programmes/Cyber-Americas/INTERPOL-Cybercrime-Capacity-Building-Project-in-Latin-America-and-the-Caribbean/Regional-approach.

Li, Xingan. "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." *Webology*, Webology, www.webology.org/2007/v4n3/a45.html.

Kennedy, Gabriela, and Karen H. F. Lee. “Data Security and Cybercrime in China.” *Lexology*, 18 June 2018, www.lexology.com/library/detail.aspx?g=6a51305a-eccd-4f3f-a3a4-0b9e21843c19.

agustina.diaz-rhein. “United Nations Office on Drugs and Crime.” *Global Programme on Cybercrime*, www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.