Research Report

Forum: United Nations Office on Drugs and Crime

Issue: Strengthening international cooperation and capacity-building efforts to combat cybercrime

Student Officer: Rashika Naganasoore

Position: Deputy Chair

LMUNA

Lorentz Lyceum
Model United Nations
Arnhem

Introduction

Cybercrime, a range of illegal activities executed through digital means, which pose an increasing threat to the stability of the economy and global security. Scoping from identity theft and financial fraud to more increasingly harsh forms of cyber terrorism, the complexity of these crime cases are drastically evolving.

As technology develops, our digital means are capable of capturing, processing and analyzing even more data. This becomes a global issue threatening the security, and economy of many nations. Criminals in this field called cybercriminals take advantage of these advancements ("History of Cybercrime").

This report will discuss the various challenges of cybercrime, and proposes measures to combat cybercrime.

Definitions of key terms

Cybercrime

Illegal activities that are carried out through digital devices, computers and networks. Cybercrime has no borders, and therefore it can be easy for cybercriminals to access victims from across the globe.

Capacity-building

Process of developing and strengthening skills to effectively "produce, perform or deploy". This can be done internationally, and on a local level depending on what the goal is. The process refers to empowering resources to adapt as well as thrive in a fast-changing world.

International Cooperation

A global collaborative relationship to work towards the betterment of an objective.

Exploit

A code or program that was exploited means that it is designed to take advantage of a flaw in a security system or vulnerability in a computer's application.

Enumeration

The process of extracting information such as IP addresses, usernames and confidential protocols and with the objective of breaching their network.

Cybersecurity

The system and process of protecting applications on computers and combating digital attacks.

Digital Forensics

A department within forensic sciences that specialize in the analyzing of security breaches, data leaks and overall protection of applications.

General overview

The spread of cybercrime has rapidly become a massive issue, especially in this current developing generation. Due to the borderless nature of cyber access, cyberattackers can use this to their advantage to interfere with systems from across the globe. It is essential for international cooperation to take place to effectively combat cybercrimes (“Cybercrime Interpol”).

The main cause of increased cybercrime is due to the rapid development of technology. Cybercrime has been recognized since the early 1980s where transcripts of personal emails were shown, however with the advanced technology of this age, there is a variety of confidential information that can be leaked (“History of Cybercrime”). With new AI software and untraceable innovations, face detection, identity theft, phishing and other types of cybercrime have become common in this industry (“Cybercrime Causes and Measures”). Moreover, cybercrime originated from France when two men broke through hacking a telegraph system for financial market information back in the early 1830s. However, since then, nations like China and Russia have been affiliated with many complaints of cybercrime according to the UNODC (“Cybercrime”).

There are many reasons why cybercrime occurs, for example for financial gain. Hacking other systems such as bank accounts will gain access to money and passwords which can be sold to the black market. Data from companies can be traded in illegal markets for advantage in market competition. Politically speaking, cybercrime is used to belittle other governments, nations and political parties. By proving that other ideologies are weaker, it shows that they are the strong choice. With the lack of international cooperation, global crimes can take place easily due to the borderless nature of the digital world (“Cybercrime Causes and Measures”).

The growing threat of cybercrimes has become a worldwide issue. According to the statistics shown at the end of 2022, data shows that 50% of businesses in the United Kingdom have suffered from a form of cybercrime. This raises a concern of national and economic security as it has put hundreds of companies in dangerous and vulnerable places.

On average, businesses spend around $4.35M to fix data breaches in the year 2022. As years go by, the technological advancement of these cybercrimes will solely increase, therefore increasing the spending amount of businesses if attacked. This presents challenges economically especially in capitalistic nations where individuals heavily depend on their businesses.

Additionally, every 1 in 2 Americans on the internet with accounts have had their data breached in 2021. This means that half of the nation has struggled with a global problem which threatens their personal information, keeping them in a vulnerable position. With this information, criminals have access to easily financially exploit companies for their gain, steal personal data for identity theft to for example pay off loans, or go by another name. The most common use of information is to sell it on the black market or other illegal markets for a financial reward ("Cyber Crime").

There are multiple types of common cyberattacks, for instance, phishing, ransomware, espionage and identity theft. Phishing is a type of software engineering which gathers sensitive information such as IP addresses, passwords and personal emails ("Cybercrime Interpol"). Another type is ransomware, where hackers can block access to certain accounts, and documents until the victim has made a payment, this is also called ransom payment. Other variants include espionage, the process of spying as a form of gathering information for their government, community or business ("Hackers Think in All Directions"). Lastly, another common type of cybercrime is identity theft, where the cybercriminal impersonates the victim to gain access to bank accounts, personal emails and their other applications which include financial fraud ("Commerce in the Shadows"). One of the most famous and impacted data breaches happened through a 4 year long course to Yahoo (Matthews).

The global impact cybercrime has is proliferating on a yearly basis. The revenue of the cybercrime industry per annum is close to $1.5 trillion, however the global cost of cybercrime is estimated to reach $10.5 trillion ("Cybercrime to Cost the World"). This amount exceeds the revenue of drug trafficking, becoming the one of the most profitable industries in the black market ("The Latest Cyber Crime Statistics"). The FBI and other agencies have received over a million complaints regarding their safety digitally in the past year. According to sources, approximately $7.1 billion has been lost allegedly due to cybercrimes, however, this is solely the reported amount, the unreported cases can increase this number ("Cyber Crime | Federal Bureau").

Essentially, cybercrime has become a norm in this digital world. Millions of people around the globe have accepted these illegalities as for them, there is no proper way to prevent it after the hacker has taken over their application ("Hackers Think in All Directions").

According to a survey conducted, approximately 30% of participants had never heard of MFA (Multi-Factor Authorization) (“Cybercrime to Cost the World”). This is a crucial security measure to take when creating an account to prevent identity theft, and other forms of cybercrime. Primarily, this type of authorization asks to sign into an account using another application such as an email, or phone number message code to confirm the log in within a time limit (“Cybercrime”).

To conclude, the hardships that businesses, governments, communities and individuals face on a day-to-day basis are evoking stripping their privacy from them. Therefore, through international cooperation and capacity-building, efforts must be strengthened to combat cybercrime.

Major parties involved

UNODC

The United Nations Office of Drugs and Crime specializes in the prevention of crime and combating drug issues like drug trafficking. They are responsible for the terrorism implications presented by the United Nations. They promote assistance for national security systems.

Interpol

International Criminal Police Organization is a committee that facilitates help globally to police. This organization offers officers a range of operational and technical support.

Cybercriminals

These are criminals that work in the cyber field. They illegally access the victim's personal information and other sensitive data.

State-Sponsored hackers

State sponsored hackers are affiliated usually with the government and other businesses to conduct espionage, cybercrime and other digital illegal activities. These organizations include the Lazarus group which is allegedly associated with the North Korean government to hack into other countries' systems. Other examples include the PLA Unit 61398 which reportedly is connected to the Chinese government, and Fancy Bear, purportedly associated with the Russian government.

Cyber Services

Groupsich reportedly is connected to the Chinese government, and Fancy Bear, purportedly associated with the Russian government.

Timeline of Key Events

1980s	Start of cybercrime through leaking transcripts of personal mails
2004	UNODC launches a global programme on Cybercrime
2013	UN resolution on digital privacy
2013	Yahoo! Data breach
2023	Present and ongoing UN discussions and negotiations on cybercrime

Previous attempts to solve the issue

UNODC

The UNODC has been sending funds to developing countries to help sort out as mentioned before to countries like Libya, Morocco and Tunisia. The equipment and training being given has gradually led to indications of possible threats which poses a positive impact in cybersecurity. These advanced equipment include digital tools to strengthen security systems to therefore diminish and stop cybercrimes. However, this is not enough as there are multiple other countries who are in need of funds and forensic equipment to combat cybersecurity ("United Nations Office on Drugs").

There have been various NGOs, UN funded organizations and businesses trying to put efforts to combat cybercrime. For example, the UNODC (United Nations Office of Drugs and Crime) funds multiple countries to prevent cybercrime like Tunisia and Morocco. These funds include the sending technologically advanced systems to identify cybercrime, as well as forensic devices. As an aim, the UNODC wishes to achieve SDGs (Sustainable Development Goals) 16 (Peace, Justice and Strong Institutions) and 17 (Partnership for the Goals) ("Cybercrime").

Implication of MFA (Multi-Factor Authorisation)

The introduction and implication of MFA (Multi-factor authorisation) was an attempt to enhance security features in multiple applications. The aim as previously stated and still ongoing is to connect to active accounts or devices like phone numbers to confirm and authorize an identity logging into an account. However, due to technological advances, cybercriminals have found ways to pass this security block seamlessly, without any trace. This is usually done by phishing, a method where a criminal tricks a victim into giving valuable information such as account passwords and card numbers as well as fake emails with the purpose of luring ("Cyber Crime").

Possible solutions

A crucial solution is to create awareness programs and educate through social media and school curriculum. This would include telling people how to prevent cyber crimes and what dangers it might cause.

Another solution is to create joint task forces internationally that will help combat cybercrime by strengthening police platforms. A way of doing this is creating a training program for operational police officers in that country.

Lastly, another solution can be to create advanced detection systems where applications can identify when their system can crash, data can be stolen, or compromised. There can be training centers for experts in the software engineering field who specialize in cybersecurity operating these training facilities.

Further reading

A crucial website to find more statistics and information about this issue can be found on the official UNODC site. This website holds up to date data regarding cybercrime in various regions globally Additionally, it provides unbiased articles that present the foundation of cybercrime. The following link will be redirected to the website: https://www.unodc.org/

Another important source read through is the Interpol website, a international police organization specializing in diminishing and combating various issues. With this link, the page will automatically take you to the cybercrime section of Interpol: https://www.interpol.int/en/Crimes/Cybercrime

Additionally, looking at your delegation's official government website regarding cybercrime can be productive initiatives to start research.

Bibliography

“Commerence in the Shadows”: Exploring Dark Web Black Markets.” *Law and World*, vol. 10, no. 2, 30 June 2024, pp. 163–183, lawandworld.ge/index.php/law/article/view/534#:~:text=There%20are%20many%20other%20types,to%20achieve%20their%20desired%20objectives., https://doi.org/10.36475/10.2.14.

“Cyber Crime | Federal Bureau of Investigation.” *Federal Bureau of Investigation*, 2024, www.fbi.gov/investigate/cyber.

“Cybercrime Interpol.” *Interpol.int*, 2022, www.interpol.int/en/Crimes/Cybercrime.

“Cybercrime.” *United Nations : UNODC ROMENA*, 2021, www.unodc.org/romena/en/cybercrime.html.

“Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” *Cybercrime Magazine*, 21 Feb. 2018, cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

“Cybercrime Causes and Measures to Prevent It.” *GeeksforGeeks*, GeeksforGeeks, May 2020, www.geeksforgeeks.org/cybercrime-causes-and-measures-to-prevent-it/.

“Hackers Think in All Directions. End-To-End Security Is the Answer.” *Cisco*, Jan. 2024, www.cisco.com/site/in/en/learn/topics/security/what-is-cybercrime.html#jump-anchor-3

Khadas, Hasina Masud. “The Causes of Cyber Crime.” *Volume 5 - 2020, Issue 8 - August*, vol. 5, no. 8, 25 Aug. 2020, pp. 476–478, https://doi.org/10.38124/ijisrt20aug432.

Matthews, Kayla. “IOTW: Multiple Yahoo Data Breaches across Four Years Result in a $117.5 Million Settlement | Cyber Security Hub.” *Cyber Security Hub*, Cyber Security Hub, 7 Oct. 2019, www.cshub.com/attacks/articles/incident-of-the-week-multiple-yahoo-data-breaches-across-4-years-result-in-a-1175-million-settlement.

“Cyber Crime.” *Nationalcrimeagency.gov.uk*, 22 July 2024, www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime.

“The Latest Cyber Crime Statistics (Updated July 2024) | AAG IT Support.” *AAG IT Services*, 17 July 2024, aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Nearly%201%20billion%20emails%20were,their%20accounts%20breached%20in%202021.

“United Nations Office on Drugs and Crime.” *United Nations : Office on Drugs and Crime*, 2021, www.unodc.org/.

“History of Cybercrime | Arctic Wolf.” *Arctic Wolf*, 19 Apr. 2024, arcticwolf.com/resources/blog/decade-of-cybercrime/

#:~:text=Technically%2C%20the%20first%20cyber%20attack,until%20the%20late%20220th%20century.