UNODC
United Nations Office on Drugs and Crime

United Nations Office on Drugs and Crime

TOPIC A:

Rising Cybercrime During the Coronavirus Pandemic

Undersecretary:
Paulina Cruz Tamayo

INTRODUCTION

As referred to by the United Nations Office on Drugs and Crime (UNODC), cybercrime "is an evolving form of transnational crime. The complex nature of the crime as one that takes place in the borderless realm of cyberspace is compounded by the increasing involvement of organized crime groups" (n.d.). While there is not an international definition for what cybercrime is, the following breaches are what it comprehends: "i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights" (UNODC, n.d.). Countries all around the globe have been severely affected by this deep-rooted issue; however, it seems to be most persistent in China, Brazil, Russia, Poland, Iran, India, Nigeria, Vietnam, USA, and Germany, respectively.

BACKGROUND RESEARCH

While it is true that this has been an ongoing topic of concern for several years now, the unprecedented and devastating Coronavirus pandemic has further aggravated it, and has exacerbated all kinds of previous situations detrimental to society. This unpredictable situation allowed criminals all over the world to successfully adapt and take advantage of people's need for reliable information, while also targeting children for grooming and exploiting purposes (Europol, 2020). Different from past years, cybercriminals in 2020 went from targeting small companies and individuals to governments and big businesses, mainly due to their weak data protection systems under these circumstances.

According to an INTERPOL report conducted between January and April 2020, "907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs — all related to COVID-19 — were detected" (INTERPOL, 2020) within this four-month period alone. Phishing emails have long been the biggest menace in this field, but this does not mean that they are the only form of malicious campaigns. UNODC's COVID-19: Cyber Threat Analysis found that among the most widely used ones, there is disruptive malware, data harvesting malware, malicious domains, online Child Sexual Exploitation (CSE) and online Child Sexual Abuse Material (CSAM) (2020). "From February to March 2020, Palo Alto Networks, one of INTERPOL's private partners, detected a 569 per cent growth in malicious registrations, including malware and phishing; and a 788 per cent growth in high-risk registrations, including scams, unauthorized coin mining, and domains that have evidence of association with malicious URLs" (INTERPOL, 2020).

While several countries and companies around the world have invested in better security systems and data-protection softwares, these still fail to fully protect people from engaging with and sharing fake news and malicious domains. As society is further relying on social media platforms for daily activities, such as communicating with family members, shopping, and reading the news, they become more vulnerable to cybercrime attacks. WhatsApp has seen an increase of 51% in usage, Facebook's interaction time increased 40%, and group calls time saw an increase of 1,000%. The latter increment explains the reason as to why cybercriminals have also been attacking through Zoom calls and video chats during the last months, often leaking personal data from the participants.

Though several studies show that the majority of people around the globe are generally aware of the fact that social media might not be the best source of reliable information, there is still an 11% of the consumers who consider these platforms to be trustworthy. It is of utmost importance to reduce this figure, as even the smallest numbers can grow into alarming statistics.

UNITED NATIONS INTERVENTION

In 2011, the General Assembly (GA) requested the United Nations Office on Drugs and Crime (UNODC) to establish an open-ended intergovernmental expert group in response to cybercrime. This expert group aimed "to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime" (UNODC, n.d.). Additionally, UNODC's Global Programme on Cybercrime, established in 2013 and funded by Canada, Japan, Australia, the United Kingdom, Norway, and USA, also aims to "respond flexibly to identified needs in developing countries by supporting Member States to prevent and combat cybercrime in a holistic manner" (UNODC, n.d.).

POINTS TO CONSIDER

- Cybercrime attacks have seen a noticeable increase during the Coronavirus pandemic due to the directly-related increase in social media platforms and internet-based appliances.
- Both developed and developing countries are highly susceptible to said attacks, which proves that it is a deeply-rooted issue all around the globe and that everyone is a possible victim.
- The United Nations has discussed this ongoing topic since 2011, which is why resolutions, such as the General Assembly resolution 65/230, and programmes have been established to respond in the best way possible.

QUESTIONNAIRE

A. What is my country's position?
B. What are my country's policies?
C. What can my country do to solve this issue?
D. Which countries can my delegation work with?
E. What are three possible solutions?
F. What has been done to solve the problem?

USEFUL LINKS

- United Nations Office on Drugs and Crime – Cybercrime: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
- INTERPOL – COVID-19 Cybercrime Analysis Report - August 2020: https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf
- Europol – Internet Organised Crime Threat Assessment 2020: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
- UNODC – COVID-19: Cyber Threat Analysis: https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf

BIBLIOGRAPHY

- “Cybercrime: Global Programme on Cybercrime”. (n.d.). UNODC. Retrieved from: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
- “COVID-19: Cyber Threat Analysis”. (May 10th, 2020). UNODC. Retrieved from: https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf
- “Internet Organised Crime Threat Assessment 2020”. (2020). Europol. Retrieved from: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
- “CYBERCRIME AND COVID19: Risks and Responses”. (April 14th, 2020). UNODC. Retrieved from: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
- Sheng, E. (July 29th, 2020). Cybercrime ramps up amid coronavirus chaos, costing companies billions. CNBC. Retrieved from: https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html