Committee: United Nations Office on Drugs and Crime (unodc.tigrismun@gmail.com)

Topic: Tackling the issue of cybercrime amidst COVID 19 pandemic and its long lasting effect

---

Letter from Dias

Dear Delegates, It is our esteemed pleasure to welcome you all to the United Nations Office on Drugs and Crime at Tigris Model UN 2022. This conference aims to provide a unique and cross-cultural experience through the unification of student delegates from around the world. We wholeheartedly embrace the objective of Model United Nations and strive to provide an enriching platform that will allow bright students to innovate solutions to our world's greatest issues. This Background guide will never be enough for research, however it will give you insight to the agenda. The Dais encourages you to research further about the agenda, foreign policies and intricate details. We hope that every delegate has a great time during the conference. An MUN is not only debating and knowledge but also meeting new people, fostering friendships, learning new things and having a time to remember. Feel free to drop your queries to the Executive Board. If this is your first MUN, it is highly encouraged that you attend the Training Session, contact the dais in case of doubts about workings of the committee. Just to conclude, the background guide aims to make an effort to give delegates a better understanding of the agenda and give them a base to build their research upon. Looking forward to seeing you all in committee!

Regards,
Aarav Gupta
Aagastya Jaipuria
Tanmay Gupta.

Overview of Committee:

The United Nations Office on Drugs and Crime (UNODC) has a mandate to assist UN member states to combat transnational crime, including corruption, human trafficking and people smuggling, drug-use prevention and treatment, drug trafficking and terrorism. UNODC's work encompasses a wide range of development-related efforts. UNODC's mandate is to combat transnational crime, including corruption, human trafficking and people smuggling, drug-use prevention and treatment, drug trafficking and terrorism. It is important to note that UNODC is not only a development agency although many of its programs provide development-related benefits. UNODC works to educate people throughout the world about the dangers of drug abuse and to strengthen international action against illicit drug production and trafficking and drug-related crime. To achieve those aims, UNODC has launched a range of initiatives, including alternatives in the area of illicit drug crop cultivation, monitoring of illicit crops and the implementation of projects against money laundering.

UNODC also works to improve crime prevention and assist with criminal justice reform in order to strengthen the rule of law, promote stable and viable criminal justice systems and combat the growing threats of transnational organized crime and corruption.

Introduction to Agenda:

The coronavirus pandemic (COVID-19) which started in 2019 quickly became a global crisis event, resulting in the mass quarantine of 100s of millions of citizens across numerous countries around the world. At the time of writing, the World Health Organisation (WHO) Coronavirus Disease (COVID-19) Dashboard reported over 7.5 million confirmed cases and in excess of 430,241 deaths globally. As COVID-19 spread across

the globe, it also led to a secondary significant threat to a technology-driven society; i.e., a series of indiscriminate, and also a set of targeted, cyber-attacks and cyber-crime campaigns. Since the outbreak, there have been reports of scams impersonating public authorities (e.g., WHO) and organisations (e.g., supermarkets, airlines), targeting support platforms, conducting Personal Protection Equipment (PPE) fraud and offering COVID-19 cures. These scams target members of the public generally, as well as the millions of individuals working from home. Working at home en-masse has realised a level of cyber security concerns and challenges never faced before by industry and citizenry. cyber criminals have used this opportunity to expand upon their attacks, using traditional trickery which also prays on the heightened stress, anxiety and worry facing individuals. In addition, the experiences of working at home revealed the general level of unpreparedness by software vendors, particularly as far as the security of their products was concerned.

Key Terms:

Cyber Crime

Use of technology, computers, or internet for illegal purpose

Dark web

Part of the internet, that is not accessible to standard search engines and is used to carry out illegal and criminal activities. Example- Tor Browser

Encryption

Hiding or protecting something using a certain secretive code or password.

Hacker

Someone who pursues knowledge of computer and security systems and uses it for criminal activities such as breaking into a system or destroying data

Piracy

Illegal copying of software that is copy-right protected

Spoofing

disguising one computer user as another

Trojan Horse

A program that contains a code to access information or systems without the user's knowledge

Key Issues:

With the onset of the pandemic and all work shifting online, cases of cybercrime have increased by a hazardously significant amount. One of the prime reasons for this today is data breaches

Data breaches:

Due to the shift to an online medium, even basic amenities are now available online on a variety of websites. These websites ask for our email address, phone number, certain personal details and sometimes also ask us to create a secure password, but is this data secure? The answer is not completely due to data breaches

A data breach is several hackers who steal all this information from the servers of these companies, even the heavily secured larger companies such as Facebook, Yahoo have suffered major data breaches wherein the information of their users got leaked onto the dark web, giving hackers their complete access. To detect these breaches websites such as haveibeenpwned have come up, but they still do not provide a complete solution to these problems, delegates are advised to come up with a comprehensive to help safeguard these details of the users and prevent data breaches.

Sextortion cases:

Yet another type of cybercrime that has become very popular nowadays is sextortion. In this hackers use a fake email, usually one having the name of the person they are threatening to send an email to. This email blackmails the person that their email has been infected with a virus (such as trojan) which gave the hacker access to their webcam and all other details. The hacker claims to have personal videos of the person and threatens to leak them to their family, friends, and colleagues. They demand a certain amount (Generally found to be between $500-$2000) in bitcoin. They choose bitcoin because it cannot be tracked in any way. In reality, these users do not have any videos or photos of the person and do not have access to their devices, it is merely just a threat however the way it is written makes the reader frightened.

Many people have transferred money to the hacker in fear, but all it did was make them lose their hard-earned money. Even if the hackers had the money there is no guarantee that the hacker will delete your video, therefore transferring them the amount they demand will not be a solution in any case.

Net Banking Funds Fraud

With the rise of e-commerce and online net banking, there is a risk that the transactions made might be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited. In addition to this, people have reported receiving calls from people claiming that they work in their bank and require their pin or OTP or CVV or any other secure information, using this, they access your bank account and rob all the funds

It is to be noted that the bank will never ask for such details over the phone, before sharing these details it is extremely important to verify the number before divulging any personal credit card or bank details. These cases of fraud are not only with the private banks but also with the public/ government-controlled banks. As representatives of various countries, delegates are recommended to debate upon this issue and decide a security measure that can be taken up to avoid such frauds.

Threat to young children:

The issue of growing cybercrime does not stop just here, in the growing technological era young children also have access to smartphones and laptops, and with a shift to online classes and school, they spend a large part of their day in front of the screen. As young children, most of them are unaware of the threat that the internet possesses. Opening of unprotected random links by these children is a cause for concern. These links and documents are hacked and opening them gives the hacker complete access to the device, and causes several cases of cyber-crimes.

Major Parties Involved:

United Nations:

The Global Programme is designed to respond flexibly to identified needs in developing countries by supporting Member States to prevent and combat cybercrime in a holistic manner. The main geographic nexus for the Cybercrime

Programme in 2017 are Central America, Eastern Africa, MENA and South East Asia & the Pacific with key aims of:

- Increased efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime, especially online child sexual exploitation and abuse, within a strong human-rights framework;
- Efficient and effective long-term whole-of-government response to cybercrime, including national coordination, data collection and effective legal frameworks, leading to a sustainable response and greater deterrence;
- Strengthened national and international communication between government, law enforcement and the private sector with increased public knowledge of cybercrime risks.

The F.B.I:

Malicious cyber activity threatens the public's safety and our national and economic security. The FBI's cyber strategy is to impose risk and consequences on cyber adversaries. The FBI is the lead federal agency for investigating cyber attacks and intrusions. They collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities, wherever they are. The F.B.I have single handedly protected thousands of citizens from various cybercrimes as well as impose appropriate punishments to those caught in the act.

Possible solutions:

Cybercrime has been an issue ongoing for a very long time and despite the numerous solutions put forth, the cases and the intensity of the issue keeps on increasing drastically. Here are some possible solutions-:

1) Laws should apply to cyber-crime—National governments still are the major authority who can regulate criminal behavior in most places in the world. So a conscious effort by the government to put laws in place to tackle cyber-crimes would be quite necessary;

2) A global culture of Cyber security needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies;

3) Establishment of an institutional framework that will be responsible for the monitoring of the information security situation at the national level, dissemination of advisories on latest information security alerts and management of information security risks at the national level including the reporting of information security breaches and incidents;

Bibliography:

https://www.unodc.org/unodc/en/cybercrime/index.html

https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

https://news.un.org/en/tags/cybercrime

https://www.un.org/en/chronicle/article/fighting-industrialization-cyber-crime

https://idn-wi.com/united-nations-definition-cybercrime

https://www.un.org/en/un-coronavirus-communications-team/un-tackling…