Committee: UNODC

Topic B: Ensuring the location of cybercriminals to lead to cybercrime eradication.

Chair: María Gabriela Dávila Martínez

Moderator: Ariadna Valdés Saucedo

United Nations Office on Drugs and Crime (UNODC) is a global leader in the fight against international crime, illicit drugs, and terrorism. It was established in 1997 through a fusion of the United Nations Drug Control Programme and the Centre for International Crime Prevention. It is made up of 500 officials worldwide. Its headquarters are located in Viena, while 20 extra offices are operating all around the world, these are located in more than 150 countries, their link offices are located in New York and Brussels.

UNODC is in charge of educating people all around the world about the dangers of drug abuse and strengthening the intervention against trafficking and production of drug-related crime and trafficking of illicit drugs. In the Millennium Declaration, Member States concluded that they needed to follow some alternatives to intensify efforts, they decided to fight transnational crime in all its dimensions, to strengthen the efforts of implementing the commitment to counter the world drug problem and to take action against terrorism. To achieve these objectives, UNODC has launched a series of initiatives, including alternatives for the cultivation of illicit drugs, the surveillance of illicit crops and the execution of anti-money laundering projects.

UNODC also focuses on improving crime prevention and assists in the reform of criminal justice to strengthen the rule of law, it promotes stable and viable criminal justice systems and combats the growing threats of international organized crime and corruption.

In 2002, the General Assembly approved a program of activities for the Terrorism Prevention Branch of UNODC. Those activities focus on assisting States that so request, for the ratification and application of the 19 universal legal instruments against terrorism, these instruments were created in the year 1963 to prevent terrorist attacks.

According to the Merriam Webster Dictionary “Cybercrime is a criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit or manipulate data.” According to the UNODC website, “Cybercrime is an evolving form of transnational crime," it is caused by the increasing number of organized crime groups. Because of the daily usage of technology, this activity has been increasing, it has been affecting the government, corporations and many people's lives, that is why UNODC is taking action, they are creating efficient and effective ways to eradicate this problem, there are criminals and victims all around the world and this has affected societies from many regions.

Catching the criminals has become a more difficult activity due to the different complications. For example, most of the time criminals do not use their personal computers to hack another system because they already know that they are being traced and they want to protect themselves, they already have a user to blame in order to avoid the problems of getting caught and arrested. Hackers use a VPN to cover the original IP address which makes them invisible, hackers also move the packages from one server to another, this makes it harder for the cyberpolice to track the information. Finally, they use new encrypting technologies that make it harder for other agencies to crack into them.

Some of the issues that The International Journal of Advanced Research in Computer and Communication Engineering Website mention are the following:

- Hacking: It is an illegal intrusion into a computer system or/and network. Hackers use special computer programs to commit this crime. The most common hacks can be stealing credit card information or transferring money from other accounts to theirs.

- Child Pornography: Children are also being damaged by cybercrime, many children have access to the internet and as it is the main tool for this crime, they tend to fall into pedophiles hands and this is were aggressions start. Pedophiles do what they want with children once they have their trust, and it is very easy for children to fall into their hands. Once they get to that point, pedophiles start distributing pornographic material so children start sharing pornographic material too, hackers commonly sell that material to make money. Many parents and educational institutions know the consequences of not following certain rules while using the internet, but many others do not know what will happen if those rules are not followed, pedophiles take advantage of those situations in which parents or teachers did not accurately advise children to prevent danger. Pedophiles follow certain tactics to operate effectively, some of them are: using a fake identity, befriending children or/and teenagers, winning their trust, extracting personal information, among others.

- Phishing: It consists of sending false messages via email and claiming to be an established legal enterprise. This is used to get personal information from the victim such as passwords, social security numbers, credit cards or bank accounts.

- Denial of service attack: This type of attack is based on sending the user a lot of e-mails to crash the user’s computer, this type of attack can be made through big packets of information or a lot of packets that the computer will not be able to handle.

- Virus Dissemination: A Software that gets into the computer and its components, and affects it from the inside-out. It can damage and even destroy the computer’s components.

- Software Piracy: Copying other software programs and distributing products by making them appear as the original ones.

- Credit Card Fraud: Using a credit card without the owner’s authorization.

- Net Extortion: Is using the information retrieved from some company to obtain by force some kind of profit.

The ENISA Threat Landscape Report 2018, states that information theft, loss, or attack is now the prevalent type of crime against organizations.

The AV-Test states that there were 137.5 million new malware samples in 2018, and currently we are already in 24.55 million as of April 2019.

According to the Webroot Threat Report in 2018, 93% of malware observed could change its code and appearance to avoid getting detected by antiviruses, and that 50% of devices that were once infected, got infected another time within the same year.

The University of Maryland researched that malicious hackers are now attacking computers at a rate of 1 attack every 39 seconds.

Imperva 2019 Cyberthreat Defense Report states that 78% of surveyed organizations were affected by a successful cyber-attack in 2018. Also, it collected several information from cyber-attacks and presented the percentages from successful attacks per year, in 2015 70.5%, 2016 75.6%, 2017 79.2%, 2018 77.2% and 2019 78.8%.

Currently, in the United States, the FBI has the Internet Crime Complaint Center (IC3), where people can go and complain about these type of crimes. This generates a friendly and safe environment where people satisfy their security needs and get the attention they need. As more people insert more information in this website, the job for the FBI will be easier because they could join information from different crimes and link them to find one of the perpetrators. They also count with a Recovery Asset Team which focuses on getting back the money that has been stolen, they have a 75% per cent recovery rate out of the cases that they have worked in.

As we already know, cybercrime is a current and existing problem and will continue to grow faster and faster as more technologies are being created, also as time goes by more people have access to a computer and sometimes they do not know the risks that it can present. That is why the UNODC is trying to find the best possible solutions to eradicate this problem or at least diminish it, there are several possibilities in order to get to this objective, such as educating the people to know all the risks of having a computer, so that they can use it without the risk of getting scammed or tricked by someone else. Also, taking harder measures on the hackers, this would make them feel more scared if they get caught and will make fewer people try and hack or plant malware in other software. Also, tracing the money, big hacking groups want to profit out of these activities, this leaves a money trail behind that will always lead to a final account where all the money is, taking advantage of this money trail can lead us to find the hackers. And of course, as obvious as it sounds catching more perpetrators, this can be done having a person inside of these groups and investing more money on the cyber police so they can be more effective.

Resources and helpful sites

COUNTER TERRORISM. (n.d.). Retrieved from https://www.un.org/en/counterterrorism/legal-instruments.shtml

Nancy.cao. (n.d.). United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org/unodc/en/about-unodc/index.html

International Journal of Advanced Research in Computer and Communication Engineering (2014) PDF https://ijarcce.com/wp-content/uploads/2012/03/IJARCCE3D__s_abdulla_Cybercrime.pdf

Cybercrime. (n.d.). Retrieved from https://www.merriam-webster.com/dictionary/cybercrime

300 Terrifying Cybercrime & Cybersecurity Statistics [2019 EDITION]. (n.d.). Retrieved from https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Cybercrime deterrence: 6 important steps. (2015, January 20). Retrieved from https://www.welivesecurity.com/2015/01/20/cybercrime-deterrence-6-important-steps/

Greene, K. (2012, October 22). Catching Cyber Criminals. Retrieved from https://www.technologyreview.com/s/405459/catching-cyber-criminals/

How can I trace a cyber criminal? (2017, July 27). Retrieved from https://www.quora.com/How-can-I-trace-a-cyber-criminal

Sanctioning Cyber Crime: The New Face of Deterrence. (n.d.). Retrieved from https://www.cfr.org/blog/sanctioning-cyber-crime-new-face-deterrence