Letter from the Chair

Dear Delegates,

It's with great pleasure and excitement that I welcome you to OMUN 2022! My name is Justin Lee and I'm excited to serve as your chair for the UNODC committee on Cybercrimes. I, along with my vice-chair Cole Herman, extend our warmest welcome to you for what we are confident will be a weekend of robust debate. I am currently a Grade 12 student at UCC, from Toronto, though I moved from South Korea in 2015. I've been involved in MUN since grade 9, and am grateful to have been given the opportunity to take part in planning OMUN this year. My passion for Model UN has been a significant part of my life for many years, attending various conferences like HMUN, BMUN, and SSUNS, and I'm excited to share my passion with all of you at this conference.

Hi, I'm Cole and I am currently a Grade 11 student at UCC. MUN has always been a passion of mine and I've been lucky to be able to attend great conferences as a team. MUN is a conduit for skills and experience as it has helped my confidence, negotiating ability and awareness of our global landscape. I can't wait to share these skills and experiences with you during OMUN.

Our committee will focus on two overarching topics that are key in the UNODC's involvement in cybersecurity. Firstly, we'll look at "Online Compromisation and Security," exploring the dimensions of phishing, cyberattacks, malware, etc. Second, we'll explore "Policing the Dark Web," where we will investigate the nature of the Dark Web and strive to produce an action plan as an international organisation on how to regulate and establish guidelines and boundaries for the Dark Web to ensure the security and safety of millions around the world. My vice-chairs and I have been working hard to put together the Background Guide with resources to help you prepare for the conference, and we hope that you are able to make use of it to its full potential. Ensure that you conduct your own thorough research, with careful attention to the backgrounds and policies of your countries.

I wish you all the best of luck in your preparations, and I greatly look forward to meeting all of you. Please feel free to reach out to me should you have any questions!

Best,
Justin Lee
Chair of the UNODC Committee, OMUN 2022
justin.lee22@ucc.on.ca

History of the Committee

The United Nations Office on Drugs and Crime (UNODC) was established in 1997 as an office under the secretariat organ of the United Nations. The office looks to combat the trade of illicit drugs, criminal justice, international terrorism, and political corruption.

Introduction

Ever since its birth on January 1, 1983, the internet grew into such an important part of everyone's daily lives. Nowadays, it seems almost impossible to imagine a life without the internet, without Wikipedia, without YouTube, without Netflix. However, with its widespread use and its accessibility, the Internet has also caused many problems for millions of people around the world. Although there have been attempts to improve the security and privacy on the Internet, the development of technology has exacerbated the use of the Internet in crimes, including, but not limited to, cyberattacks, the Dark Web, etc.

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centres and other computerized systems. Cybersecurity is crucial in protecting the daily lives of everyone around the world, especially in the status quo. During the COVID-19 pandemic period, cybercrimes rose by 600%, especially with mailing schemes disguised as CDC (Centre for Disease Control) or WHO (World Health Organization) officials regarding the pandemic. Furthermore, malware attacks have been trending upwards as well. Malware, or malicious software, is any piece of software that was written with the intent of doing harm to data, devices or to people. Types of malware include computer viruses, trojans, spyware, ransomware, adware, worms, file-less malware, or hybrid attacks. Recent malware attacks have become more sophisticated with the application of machine learning and targeted spear-phishing emails into their attacks. The total number of malware infections rose from 12.4 million in 2009 to 812.67 million in 2018.

Secondly, we will explore the intricacies of the Dark Web, which is only accessible by certain browsers, such as Tor (The Onion Routing Project), and guarantees anonymity. Granted, the Dark Web is sometimes used by those who would be endangered by revealing their identities online. Abuse and persecution victims, whistleblowers, and political dissidents have been frequent users of these sites. Nonetheless, these benefits can be easily extended to those that want to act outside of the constraints of laws in other explicitly illegal ways such as trafficking, illegal pornography, and cybercrimes.

As the UNODC, it will be important to address this issue of cybercrimes and act as a unified body to tackle this global problem in great detail. Delegates will have to explore the complexities of online anonymity, accessibility to the Internet, and harnessing its powers.

Subtopic A: Online Compromisation and Security

During the Covid 19 pandemic, a greater reliance on digital technology as well as economic vulnerability led to a massive increase in attempted cybercrime. For instance, in one week in April 2020, there were over 18 million daily malware and phishing emails related to the disease reported by a single email provider, in addition to more than 240 million COVID-19-related daily spam messages. This small-scale crime was also accompanied by larger cyberattacks as reported by a recent report of the UN Secretary-General. This rapid influx of cybercrime is dangerous for both the private citizen as well as the international community. Bad actors (Both State and Non-State) have challenged our online space in ways we could not have expected. From misinformation, leaked personal records to even the ability to cripple whole power grids, our increased digital connectivity has, in turn, led to increased access to our vital systems.

This increase poses a major risk to your information security. This is broken down into two main areas, the validity of the information you consume as well as the protection of the information you provide.
The validity of our information consumption has worsened in the last 20 years. We see declining ratings of trust in institutions, with current levels of trust number going below 40% in journalistic media. This creates the perfect climate for misinformation as it allows actors to create false narratives and attempt to influence various movements as seen prominently in recent US and European elections.

Secondly, people's personal details are at as great a risk as ever. These details are usually casualties in many cyberattacks around the world. For example, the 2013 cyberattack on Capital One released over 106 million credit card numbers leaving their customers vulnerable to theft and other crimes. This trend becomes more worrying the more data that is collected about our online and even physical activities, with companies having access to your location, messages, microphone and other personal data. This makes the need for increased security even more vital as the consequences of a breach may prove life-threatening.

A final area of concern is the growing digital divide between states. Those in the global north have the infrastructure in place to cyberattacks at both a national as well as individual level. This can take the form of Computer Emergency Response Teams (CERT) or other cybercrime units. In contrast, states who have only begun digitization are particularly vulnerable to these attacks, as they have put a lot less effort into their security. For instance, over 80 percent of countries in the Americas and Asia and Oceania reported requiring technical assistance in dealing with cybercrime. This lack of security threatens to only widen this divide and prevent global digital cooperation.

Subtopic B: Policing The Dark Web

Our lives are shaped around the internet; however, we only interact with around five percent of it in our daily lives. This space with Instagram, Google and other well-known companies is referred to as the surface web. Encapsulating most of the internet is a collection of medical records, password-protected areas and other private information surmised as the Deep Web. The main differential of the deep web is that it's not publicly available, or in other words, you need access. Finally, there is the Dark Web; a collection of intentionally obscured web pages and a vestige for illicit items and services. These include all areas of products, including drugs, stolen information and records, and weaponry. A key feature of the Dark Web is that it is only accessible through specific software, and because of this users remain anonymous and untraceable, making it very difficult for law enforcement to limit these operations. This software is typically clients like Tor and I2P. These clients use technology to encrypt the user's data and mask the IP address of the connection. Through these clients users then access specific web pages and access marketplaces where they can purchase various goods and services. These marketplaces are quite similar to the ones we use throughout our daily lives although the goods for sale tend to differentiate them. Almost all of these transactions are completed through some form of cryptocurrency to maintain the anonymity of their purchases. However, a weak link in the system arises in the transport between the buyer and seller as some information must be shared in order to ship these items. To combat this flaw, some of these marketplaces have become so advanced that they have

maintained their own private shipping services making these transactions practically untraceable. Another potential manoeuvre is for the seller to ship several perfectly legal packages and have the buyer assemble the weapon in a practice known as “ghost guns”.

Potential impacts

With their recent popularity, these sites have been able to circumvent the traditional methods of the drug and firearm trade. While these criminal areas normally lend themselves to centralized operations, bad actors now rely on these decentralized sites and vendors due to the safeties associated with these transitions. This poses a major threat to global security as these items can end up untraced and in the hands of the highest bidder. While most current gun violence still is armed through conventional sources, the potential of the black market is dangerous, as has been seen in many cases around the world. For instance, on March 4th, 2022 the student involved in the Olathe East High School shooting, used a “ghost gun” in an attempted murder. The anonymity of the weapon prevents law enforcement from taking a more active approach and curtailing illegal firearms within the county. This incident is only one of many that will continue if these illicit channels aren’t monitored.

Further Research

https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/firearms

https://crsreports.congress.gov/product/pdf/IF/IF11810

https://www.torproject.org/about/history/

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

https://www.technadu.com/silk-road/57417/

https://morningconsult.com/tracking-trust-in-institutions/

https://www.upguard.com/blog/biggest-data-breaches

https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf