Ontario Model United Nations III

International Criminal Police Organization, Background Guide

April 7th to April 8th, 2018
omun.ca

A Letter from the Chairs

Hello Delegates!

Our names are Shaan and Arjun, and we are tremendously excited to to welcome you to this year's INTERPOL session.

Model UN has taught us so much in the past few years. Even though we are both only in Gr. 10, we have been doing Model UN for about two years already and we have both had the incredibly good fortune of travelling nationally and internationally for our club. Model UN has allowed us to develop passions for the economy, the role of international law, the ins and outs of lawmaking, the art of compromise, and so much more! We hope, more than anything, that we can help to spark or further develop a passion in what we discuss over the course of our committee session this year.

INTERPOL is a global policing force (for all of it's 192 members states), with the objectives of connecting police forces to better enforce against crimes that transcend international borders within the laws that apply to individual nations and in the spirit of the Universal Declaration on Human Rights, as well as to develop and establish institutions that contribute towards the policing of ordinary crimes.

The two topics which we plan to discuss this upcoming session are both at the utmost importance and relevance for the INTERPOL community. Firstly, the topic of cybercrime - one of the largest and yet most unregulated harmful practices in the modern-day. Secondly, the topic of trafficking, with regards to humans and drugs, amongst others, is so varied in its forms that it can be very hard to police against. We are really looking forward to seeing the solutions you have come up with to tackle these challenging issues.

Position papers will be due by the beginning of the first committee session on Saturday, April 7th if the delegate should remain eligible for awards. They can be submitted through PDF by email or can be handed in with paper at the start of the first session. Position papers should be one page in length, single spaced, in Times New Roman 12 point font.

On a final note, this background guide, while it is quite information heavy, should only be a starting point for your research. We strongly recommend you try to answer the guiding questions at the end of each section and explore the links we used in our bibliography to get you started after you read the background guide! These questions will really help you develop substantive arguments in moderated caucuses as well as in the resolution drafting process.

We are so excited to see you all on April 7th and 8th this year! If you have questions, feel free to email us.

Good luck!

Shaan & Arjun
Chairs of INTERPOL, OMUN 2018
interpol@omun.ca

Topic 1: Cybercrime

Background

Cybercrime is a field that, because of its increasing capabilities in the modern day, is becoming more and more prevalent in all aspects of society. While there is lack of international agreement over an all-encompassing definition of what cybercrime actually encompasses, it is generally agreed upon that cybercrime is an illegal act performed with the use of an electronic device. These illegal acts include, but are not limited to: hacking; spreading hate and inciting terrorism; distributing child pornography; and grooming[1]. The main issue surrounding cybercrime is that it is a largely unknown space by both legislative bodies and citizens themselves. Subsequently, many citizens are left vulnerable to cybercrimes as a result of improper education and legislative protection.

Cybercrime is under the umbrella term of cyber espionage, which includes cybercrime, cyber attack, and cyber warfare. The Tallinn Manual, first published on March 15, 2013[2], provides the most globally adhered-to version of cyber espionage and the subsequent activities that fall underneath it. There are three distinct categories of cyber operations that fall under the Tallinn Manual: cyber crime, cyber attack, and cyber warfare. The most basic of the three definitions is of cybercrime, which is unique in that it is a crime committed using an electronic device but the act is for or with a government. Cyber attack differs from cybercrime in that it involves nation states as opposed to people/groups not tied to governments in any way. Cyber warfare is a group of cyber attacks whose effects must be similar in magnitude to that of a real war. As you can see, with these definitions and differentiations still in their infancy, it might sometimes be difficult to tell the three subcategories of cyber espionage apart. However, the only legislation that may be put in place under INTERPOL's jurisdiction is with regards to international policing - thus policing illegal cyber activities not tied to the nation-state.

Advanced Cybercrime

There are two categories of cybercrime: advanced cybercrime, which includes sophisticated attacks against hardware and software, and cyber-enabled crime, which qualifies as a traditional crime that can now be eased through the internet. Hacking is the most popular method of performing advanced cybercrime in this era. The exponential increase in both number and severity of cyber hacks are of recent and these trends have a strong correlation with the ever-improving and ever-more-accessible technology we are using today, but cybercrime itself has been around for quite a while. Since the first hack before even the internet existed in 1981, when Ian Murphy hacked into the AT&T network and change the internal clock to charge off-hours rates at peak times for cell use, it was easy enough to track him down, but technology and unified governmental policies were never able to match the ingenuity of one single man and

[1]Government of Netherlands, "*Forms of Cyber Crime,"* Accessed January 2018, https://www.government.nl/topics/cybercrime/forms-of-cybercrime.
[2] Michael N. Schmitt, "*Tallinn Manual*,' Accessed January 2018, https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

a phone[3]. This discrepancy between cybercrimes and cyber security is only becoming larger as technology gets better. With more and more people to be able to access the technology needed to take part in this illicit behavior, hacks are getting harder and harder to prevent. The term "hack" itself has now branched out into many subcategories: viruses; trojans; and worms - all of which are able to execute and reproduce on their own. A virus is the most fundamental of the three aforementioned categories. By definition, a virus "is a small program or script that can negatively affect the health of your computer and can create files, move files, erase files, consume your computer's memory, causing your computer not to function correctly."[4] While viruses do replicate at a virulent rate, they are not incurable. People can download antivirus programs which can protect the "immune system" of the computer from impending attacks. As the word implies, Trojans are never to be trusted because they are, in effect, imposters. Trojans masquerade themselves as regular programs such as games, disk utilities, and even antivirus programs. However, if they are run, these programs can do malicious things to your computer.[5] Worms are the hardest form of hacking to detect. They are typically considered invisible files, and they can infect your device by replicating so many times that your device can no longer function. What's more is that these worms can "travel between systems without any action from the user."[6] Hacks have a wide variety of consequences for the victim(s), ranging from identity theft to fraud to money stolen from online banking accounts, but the aforementioned three types of hacks are the fundamentals to creating a sophisticated hardware or software attack. Generally speaking, antivirus programs are the most viable solution to most of the aforementioned three forms of hacking, but what is most concerning is the general electronic device user population is lacking knowledge on how to protect their devices from infection or theft of personal information.

INTERPOL must consider what pre-existing legislation must be changed in order to better police the increasing variety and severity of hacks on the private sector and individual civilians.

Cyber-enabled Crime

While hacking is often viewed as the predominant sub-classification of cybercrime, it is important to remember that cybercrime appears in other forms, and has become a very popular method of inciting terrorism in the last decade. The inciting of terrorism is a cyber-enabled crime as people were always able to perform terrorist acts without the internet, but now are able to access another path for destruction. A good example of a terrorist group leveraging the internet to recruit new members would be the Islamic State of Iraq and the Levant (ISIL). Please note that ISIL is not being regarded as a nation-state of any sort as they have not been recognized as such by the global community. Instead, they are regarded as a terrorist organization. With the emergence of the internet, ISIL now has access to hundreds of millions of potential recruits, and the organization made news headlines when they successfully recruited hundreds of teenagers across North America and Europe, simply through social media. ISIL,

[3] Le VPN, "*Where does cybercrime come from? The origin and evolution of cybercrime,"* Published April 27, 2017, Accessed January 2018, https://www.le-vpn.com/history-cyber-crime-origin-evolution/.
[4] Tech Terms, *"Virus,"* Published August 6, 2011, Accessed January 2018, https://techterms.com/definition/virus.
[5] Tech Terms, *"Trojan Horse",* Accessed January 2018, https://techterms.com/definition/trojanhorse
[6] Tech Terms, *"Worm"*, Accessed January 2018, https://techterms.com/definition/worm.

while the acts of terrorism they perform are by no means acceptable, they have been the most "successful" terrorist organization in the last decade because they have utilized technologies around them. They use youtube videos with cats and sleek graphics to make Jihad appear to be fun. They contact teens through social media with the sole intention of getting to know each other. Then the severity of the tasks increase every time, and within a couple of months these teens are either being smuggled to Istanbul or other nearby areas to work for the organization or, worse, they might do the organizations' bidding in their own local communities[7]. While law enforcement can track these cyber-enabled crimes, it is essential that the global community feel less susceptible to commit acts of terrorism through the utilization of media and cyberspace. An important question to consider is what measures, from an enforcement perspective, can be put in place to prevent citizens from being vulnerable to terrorism.

Child pornography is another cyber-enabled crime that has risen to prominence within the past few years. This specific cybercrime is largely unlegislated and fails to have a cyber-specific definition and, therefore, there is no international agreement on what cyber-enabled child pornography even entails. In fact, 35 countries still have no anti-child pornography legislation, let alone cyber-enabled child pornography[8]. It is essential that international agreement is found in defining and separating cyber-enabled child pornography from current child pornography legislation, as well as a proper criminal prosecution for offenders under national law.

Finally, identity and information theft are often more easy to find in the cyberspace than many imagine. The main cause of easily-enabled information theft is civilians' and businesses' lack of knowledge surrounding the topic of data protection. In 2016 alone in the United States, 16 billion was stolen from more than 15.4 million consumers.[9] Approximately 5% of the American population was affected by cyber identity theft in one year. This astounding fact leaves the international community to question how civilians and businesses can be better educated to protect this sensitive information by their own national governments, as well as the international community.

The lack of legislation surrounding the aforementioned types of cybercrimes, as well as the many new types of cybercrimes that are arising every day, make it very difficult for nations to accomplish their most important task: protect their civilians. If we, as a global community, have not even come to a unified consensus in creating a definition for cybercrime, it will be very hard to find international agreement on international law enforcement. The topic of cybercrime, while seemingly far fetched and lacking physical consequences on civilians, will have monumentally destructive effects on society if left unregulated.

---

[7] Larry Greenemeier, *"When Hatred Goes Viral: Inside Social Media's Efforts to Combat Terrorism",* Published on May 24, 2017, Accessed January 2018, https://www.scientificamerican.com/article/when-hatred-goes-viral-inside-social-medias-efforts-to-combat-terrorism/.

[8] International Centre for Missing and Exploited Children, *"Child Pornography: Model Legislation & Global Review"*, Accessed January 2018, https://www.icmec.org/child-pornography-model-legislation/.

[9] Insurance Information Institute, *"Facts + Statistics: Identity theft and cybercrime",* Published January 2017, Accessed January 2018, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

Past Actions

United Nations Group on Cybercrime and Cyber Security (2017):

At its 22nd session, the High Level Committee on Programs (HLCP) created the UN Group on Cybercrime and Cyber Security. At its 24th session, the Group was tasked, under the leadership of ITU and UNODC, to develop a draft policy on cybercrime and cyber security that focused on the external dimension of the issue, in particular on how the UN system mainstreamed cybercrime and cyber security issues into programmes delivered to Member States. While this draft policy was created, it only focused on the cyber security and anti-cybercrime capacities of Member States and not on the UN's internal needs. This was the only international organization created on the issue of cybercrime to date. Nations still have very segmented and flawed cyber security strategies that must be addressed by the international community[10].

Further Research

Obviously, the ever-diversifying field of cybercrime is becoming more and more volatile with every passing minute. INTERPOL should address the following questions surrounding cybercrime in committee:

1. How can the international community come to a consensus on an international agreement of what defines cybercrime and what punishments should be enforced for those guilty of a cybercrime under international law?
2. How can INTERPOL influence/incentivize nations to adopt similar policies to those created in the international community within their own nations' borders?
3. How can INTERPOL utilize the private sector in crafting a long-term cybercrime solution? For example, how would a partnership with antivirus corporations be established to garner more information on cybercrime?
4. How can civilians and businesses be educated and supported by their respective governments on the issue of cybercrimes to reduce the number of loopholes that cyber criminals can take advantage of?
5. How can INTERPOL not only establish a policy that ensures nations can prevent and enforce against cybercrime in the present day but also establish a forward-looking framework that considers the potential expansion of cybercrime to other, developing means of technology? For example, how to take into consideration the development of artificial intelligence and its impact on cybercrime?
6. What can INTERPOL actually do? What say and enforcement abilities do they have in international and national law?
7. What is your nation's stance on cybercrime?

[10] United Nations System, "*Action on Cybercrime and Cyber Security",* Published March 5, 2013, Accessed January 2018, http://www.unsystem.org/content/action-cybercrime-and-cyber-security.

Topic 2: Trafficking

Background

According to the International Labour Organization (IRO), forced labour alone, generated over 150 billion dollars in revenue in 2014 alone.[11] IRO studies have estimated that Human Trafficking, is the quickest expanding criminal industry globally, with as many as 21 million people (in 2012) entrenched in this form of modern day slavery.[12] Although Trafficking occurs within smaller regional bodies (such as municipalities), it is an issue which has ramifications for the whole globe and is recognized as a primary issue both by the IRO and by the United Nations Convention Against Transnational Organized Crime.[13] Human Trafficking is typically divided into three distinct categories based on the nature of the labour including Forced labour, child exploitation and sexual exploitation. Of these Forced Labour is the most prominent, with approximately 68% of all Trafficking being comprised of labor. [14]

Sexual Exploitation

Sexual Trafficking is defined by UN as the "transporting or harbouring of persons by improper means (abduction, coercion) for the purpose of seuxal exploitation. Sexual trafficking is the second largest facet of human trafficking and unlike forced labour, often occurs across borders.[15] Today approximately 800,000 women and children are exploited, with the main concentration of sexual trafficking occuring in Asia, followed by Central and Eastern Europe. Sexual trafficking tends to be more prevalent in areas undergoing mass migration.[16] It is one of the largest issues plaguing refugee camps across Europe, this is because often women and young girls are left without any protection due to inadequate/corrupt security and lack of oversight in migration paths and camps. Domestically, Sexual Trafficking occurs most often within poorer areas, as the decreasing amount of economic alternatives increases the vulnerability of Women to be "tricked" or coerced into sex trafficking. Sexual Trafficking in these regions have been directly correlated to employment rates, job security and a gender-wage gap for women.[17] While some forms of trafficking are easy to spot such as prostitution, others are very well hidden and operate out of secretive locations such as brothels, spas and massage parlors in unsuspecting areas.[18] When formulating a solution to this issue, it is important that delegates not only prevent the act of Sexual Trafficking itself, but the numerous external factors and root causes, that make women and children more vulnerable to be exploited.

[11] "Economics of Forced Labour", International Labour Organization, May 20th 2014, Feb 3rd 2018, http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_243201/lang--en/index.htm
[12] "Forced Labour, Modern Slavery and Human Trafficking," International Labour Organization, September 2017, Jan 29th 2018, http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm
[13] Ibid
[14] "Human Trafficking," Wikipedia May 2005, Jan 31st 2018, https://en.wikipedia.org/wiki/Human_trafficking
[15] "Sex Trafficking," Soroptimist, Feb 1st 2018, https://www.soroptimist.org/trafficking/faq.html
[16] Ibid
[17] Ibid
[18] Ibid

Forced Labour

Forced labour, is by far the most common form of Human Trafficking, mostly due to the fact that it is by far the most profitable, generating over a hundred billion dollars per annum.[19] A startling amount of consumer goods and food products imported into western nations such as the United States are produced overseas through forced labour. Because forced labour produces goods at an increasingly low price, nations and consumers have an incentive to buy those products. This perpetuates the strength of the forced labour industry, because goods produced by forced labour are frequently bought by consumers, Traffickers have a cash incentive to continue their business.[20] In addition, goods that are produced by forced labour are often very well hidden in the supply chain and are hard to trace back to any tangible source. In an increasing age of globalization where the economies of nations are become increasingly integrated with one another, it is even easier for traffickers to enter their goods into mainstream supply chains.[21] There is a greater need now more than ever for nations to push for "ethical consumerism" and fair wages, in order to break down some of the economic incentives consumers provide to traffickers which drive the growth of the industry.[22] When coming to the resolution of this issue, delegates must consider how to destroy the profit incentives that traffickers currently have to continue trafficking people. As well to consider how we can prevent goods produced through forced labour from entering mainstream supply chains and how we can better recognize and find areas where trafficking is occuring.

Trafficking of children

The international organization for migration (IOM) estimated that in 2012, 35% of all trafficked persons consisted of people younger than 18 years of age with 215 million worldwide and over 100 million working under hazardous conditions.[23] Commercial exploitation of children is a unique form of forced labour because it can manifest itself in multiple different forms, children are coerced into doing tasks ranging from production of goods, prostitution, begging, illicit adoption, and in extreme cases being made into child soldiers.[24] Trafficking of children is very prevalent in impoverished regions with Thailand and Brazil being the countries with the worst child trafficking rate in the world. One of the reasons for this is that parents who are in extreme poverty are often taken advantage off by traffickers. Parents will often sell their own children in order to acquire more income, or be coerced into giving their children up under the guise that they will be offered a better life with traffickers.[25]

---

[19] "Profits and Poverty, the Economics of Forced Labour," International Labour Organization, Jan 28th 2018, http://www.ilo.org/global/publications/ilo-bookstore/order-online/books/WCMS_243391/lang--en/index.htm
[20] Ibid
[21] Ibid
[22] Ibid
[23] "Human Trafficking," Wikipedia
[24] Ibid
[25] Ibid

Past Actions

Supplementary Convention on the Abolition of Slavery (1956)

In 1956, 123 nations gathered in Geneva, Switzerland; for a United nations meeting discussing forced labour, lead by US president Dwight D Eisenhower. The convention decided to create an international framework, which expressly secured the abolition of forced labour of any kind. The treaty combined and ratified clauses from the 1930 Forced Labour Convention and the 1926 Slavery Convention.[26] The treaty explicitly banned any actions involving forced or compulsory labour as well as debt bondage, surfdome, child marriage, servile marriage, and finally child servitude. This was a significant step by the international community in an attempt to curtail human trafficking, as this was the first concrete legal document/framework adopted internationally to illegalize all facets of forced labour.

Council of Europe Convention on Action against Trafficking in Human Beings (2005)

On May 3rd, 2005, the Committee of Ministers of the council of Europe met in order to discuss steps that needed to be taken to end the rapid proliferation of forced labour in Europe. The Committee, signed a new, more comprehensive treaty which was focused on protection measures for victims of human trafficking, as well as the safeguarding of their rights.[27] The convention also aimed to establish robust prevention measures to lower the rate of forced labour overall. Finally it seeked to set up international mechanism in order to allow easier prosecution of trafficking perpetrators, to act both as a punishment mechanism for criminals and a further deterrent for the committing of crimes involving coercive labour. The convention set up an unbiased third party organization to act as an independent monitoring mechanism which would oversee and control the fulfillment of the clauses in the treaty.[28] This group is known as the Group of Experts on Action against Trafficking in Human Beings (GRETA). Through the treaty, GRETA has published detailed accounts of trafficking and forced labour in 17 different nations. These reports have allowed for a greater understanding of the circumstances under which trafficking is most prevalent and thus more effectively fight against it. Furthermore it has lead to numerous prosecutions of individuals/organizations which have violated the European Convention on Human rights.[29]

Organization for Security and Cooperation in Europe

In 2003, the Organization for Security and Cooperation in Europe (OSCE) further developed and integrated international structures aimed at creating political incentives for governments to dedicate resources and time to combat trafficking on a national scale.[30] In addition it aimed to rally public awareness for the issue. In order to do this, firstly the OSCE established the Office of the Special Representative for Combatting the traffic of Human Being. This group was tasked with efficiently carrying out the establishment of the goals set forth by the

[26] Ibid
[27] Ibid
[28] Ibid
[29] Ibid
[30] Ibid

OSCE. This organization created by the OSCE was effective at completing a myriad of tasks which served to reduce trafficking. This included the training and vetting of global and national agencies to help them more effectively combat trafficking in their jurisdictions.[31] In addition they ran campaigns to further the promotion of anti-corruption policies which were put in place to reduce ability of trafficking organizations to act covertly. Finally it created a system in which "special representatives" from the OSCE were able to visit nations in order aid the governments in effective implementation of any anti-trafficking policies aimed at fulfilling goals set by the nations themselves.

Further Research

It is clear that there lies a broad number of new options for nations of this committee to put forward, and may include, but is not limited to the expansion upon previously taken actions some of which are mentioned above. When conducting research for a solution, it is important that delegates not only consider all of the different sub-issues that must be dealt with within this multifaceted topic, but how well their solution aligns with their countries foreign policy. Below are some questions aimed at guiding your research

1. How do you create political will or incentives for governments to establish anti-trafficking policy, particularly in areas in which it is not thought of as a major issue?
2. How can we more effectively trace and shut down hidden supply chains which carry goods produced by forced labour?
3. How can we destroy the growing economic incentive for forced labour to continue?
4. How can we improve protection of women and children in poorer regions to ensure that they don't fall victim to sexual trafficking?

[31] Ibid

Bibliography

1. Government of Netherlands. "*Forms of Cyber Crime*". n.d., Accessed January 2018. https://www.government.nl/topics/cybercrime/forms-of-cybercrime.
2. Michael N. Schmitt. "*Tallinn Manual*". Published March 15th, 2013, Accessed January 2018. https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.
3. Le VPN. "*Where does cybercrime come from? The origin and evolution of cybercrime*". Published April 27, 2017, Accessed January 2018. https://www.le-vpn.com/history-cyber-crime-origin-evolution/.
4. Tech Terms. *"Virus."* Published August 6, 2011, Accessed January 2018. https://techterms.com/definition/virus.
5. Tech Terms. *"Trojan Horse"*. n.d., Accessed January 2018. https://techterms.com/definition/trojanhorse.
6. Tech Terms. *"Worm"*. n.d., Accessed January 2018. https://techterms.com/definition/worm.
7. Greenemeier, Larry. *"When Hatred Goes Viral: Inside Social Media's Efforts to Combat Terrorism"*. Published on May 24, 2017, Accessed January 2018. https://www.scientificamerican.com/article/when-hatred-goes-viral-inside-social-media-efforts-to-combat-terrorism/.
8. International Centre for Missing and Exploited Children. *"Child Pornography: Model Legislation & Global Review"*. n.d., Accessed January 2018. https://www.icmec.org/child-pornography-model-legislation/.
9. Insurance Information Institute. *"Facts + Statistics: Identity theft and cybercrime"*. Published January 2017, Accessed January 2018. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.
10. United Nations System. "*Action on Cybercrime and Cyber Security"*. Published March 5, 2013, Accessed January 2018. http://www.unsystem.org/content/action-cybercrime-and-cyber-security.
11. "Economics of Forced Labour", International Labour Organization, May 20th 2014, Feb 3rd 2018, http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_243201/lang--en/index.htm.
12. "Forced Labour, Modern Slavery and Human Trafficking," International Labour Organization, September 2017, Jan 29th 2018, http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm.
13. "Human Trafficking," Wikipedia May 2005, Jan 31st 2018, https://en.wikipedia.org/wiki/Human_trafficking.
14. "Sex Trafficking," Soroptimist, Feb 1st 2018, https://www.soroptimist.org/trafficking/faq.html.
15. Profits and Poverty, the Economics of Forced Labour," International Labour Organization, Jan 28th 2018, http://www.ilo.org/global/publications/ilo-bookstore/order-online/books/WCMS_243391/lang--en/index.htm.
16. "Human Trafficking," National Institute of Justice, March 27th, 2007, Jan 27th 2018, https://www.nij.gov/topics/crime/human-trafficking/pages/welcome.aspx.

17. “Committee of Ministers of the Council of Europe,” Wikipedia, April 2011, Feb 4th 2018, https://en.wikipedia.org/wiki/Committee_of_Ministers_of_the_Council_of_Europe.