INTERPOL

CYBERCRIMES

Lucas Rodrigues
Ana Clara Britto
Vitória Assis

XIII SANTA MUNDI

Index

1. The Board of Directors

Sejam bem vindos ao comitê em inglês da Santa Mundi 2018! Para permitir que os delegados se situem melhor, o guia será inteiramente escrito na língua oficial do comitê. Esperamos que vocês tenham uma ótima experiência com o comitê, e que este guia possa prepará-los adequadamente.

Good evening, Delegates. My name is Lucas Gabriel and I'm the Lead Director of this year's Interpol. I am currently majoring in Biology at the Federal University of Minas Gerais, but UN models have been a huge part of my life since high school. I have been involved in the making of the Santa Mundi model for about 4 years now, and hopefully this year I'll be able to give you the best experience possible. I look forward to meeting all of you and hope you have a good time in our committee.

Hello, Delegates. My name is Vitoria Assis and I'm an Assistant Director of this year's Interpol. I'm in the second year of high school at Santo Agostinho. It is my first time as a member of the board,

although I’m the vice director of the english committee of SIA. Hope you have a good time in our committee; we are doing our best to give you an amazing simulation.

Greetings, Delegates. My name is Ana Clara and I am an Assistant Director of this year’s Interpol. I am a Santa Marcelina student, currently on the senior year of high school. I have been part of the Santa Mundi’s crew since 2016, although this is my first time behind the Board of Directors. It will be a pleasure to meet you and I hope we all have a wonderful time in our committee.

Greetings, Delegates. My name is Laura and I’m an Assistant Director of this year's Interpol. Currently I am in my senior year of high school in Santa Marcelina. I only took part in Santa Mundi once, because I am a little bit shy, although I’m looking forward to this committee to experience the dynamics of being in the Board of Directors while speaking english, I hope you all enjoy the committee along with me, I look forward to meeting you.

2. The Internet and Its Influence

During the twentieth century, the world has benefited greatly from technological innovation, spanning from the invention of the telegraph, telephones, television and, finally, the internet. While all of these contributed decisively to the evolution of the international society and globalization, the internet, for the most part, has enabled the transfer of data between faraway places in speeds that were thought inconceivable. It has allowed for communication between different continents, without the barriers previously present.

The interconnectivity provided by the internet has proven to be beneficial to interpersonal relationships, as well as acting as a massive information database and important medium for financial transactions. In short, it conveniently provides a series of services that were limited (and in many cases wholly unaccessible) all over the world, and access to it has been recently deemed a fundamental human right.

On the other side, however, there’s a darker side to the internet. From the spread of misinformation to rampant acts of violence and cybercrime, the web has been used in several negative ways. Encompassing acts ranging from cyberbullying to fraud, cybercrime can have a tangible effect on the individual, but it should also be noted that it may also have an insidious effect on organizations and States.

In this committee, delegates are encouraged to look at cybercrime through the lens of law enforcement. As police chiefs, your job is to evaluate the ways in which the INTERPOL can act to ensure the safety of the population on the web.

3. INTERPOL

The INTERPOL (*International Criminal Police Organization*) is the world's largest international police organization, an international organization of significant size, currently counting with 192 member countries. It was created in 1923, under the name "International Criminal Police Commission", and adopted the current name in 1956.

Since adopting its new name, the INTERPOL is guided by a Constitution[1], adopted in june of 1956, which outlines INTERPOL's aims and objectives. It establishes the mandate of the Organization to ensure the widest possible cooperation between all criminal police authorities and to suppress ordinary law crimes.

The aims of the organization are established on Article 2 of the Constitution. Those are, first, to enable and ensure the cooperation between criminal police authorities through collaboration and the exchange of information, and, second, to establish infrastructure and institutions in order to suppress regular crime. Furthermore, Article 2 specifies that international police cooperation is to be conducted within the spirit of human rights, establishing the Organization's obligation to follow and respect the rights and freedoms of individuals over the course of their operations. This clause is, however, complemented by Article 3 of the Constitution, commonly referred to as the "neutrality clause", which states that the INTERPOL is strictly forbidden from staging interventions related to political, military, religious or racial questions.

3.1. Special Notices

The International Criminal Police Organization operates on a well established system of notices. These are used to convey alerts and requests for cooperation, allowing member countries to communicate and share crime related information. They are:

Red Notice: To seek the location and arrest of wanted persons with a view to extradition or similar lawful action.

Yellow Notice: To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.

1 Available for access at https://www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution

.**Blue Notice:** To collect additional information about a person's identity, location or activities in relation to a crime

Black Notice: To seek information on unidentified bodies.

Green Notice: To provide warnings and intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.

Orange Notice: To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety.

Purple Notice: To seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.

INTERPOL - United Nations Security Council Special Notice: Issued for groups and individuals who are the targets of UN Security Council Sanctions Committees

4. Cybercrime and Cyberespionage

It is considerably difficult to define the term Cybercrime. Some definitions are broader, defining it as any illicit or illegal activities committed through the use of a computer or a network, however, that definition leaves it open for more traditional crimes, such as murder, if the perpetrator were to use a piece of hardware to commit the crime. For that reason, this committee will take as reference a more narrow

approach. A more fitting definition, therefore, will be computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks (GERCKE, 2012). This definition allows us to view cybercrime both on an individual's level and in an international level.

The definition of Cyberespionage, however, is easier to give. Cyberespionage pertains to offences against the confidentiality, integrity and availability of computer data, that is, the use of global networks and hardware to intercept and acquire confidential or personal information. This can be done in a number of different ways, either through Hacking, that is, the unlawful access to a computer system, often through the breach of password security, Direct Data Acquisition through various techniques, such as phishing or physical access, and Data Interception, in which offenders attempt to intercept communication and data transfers through breaches in communication infrastructure and record information thusly.

4.1. The Budapest Convention

The Council of Europe's 2001 Budapest Convention on Cybercrime [2] is the first major international treaty to focus on crimes committed through the network. It deals mainly with infractions based on information security violation, child pornography, hate crimes, copyright infringement and fraud. Within it are contained a series of powers and procedures intent on providing guidelines for signatory nations to build legislation upon, such as on the topic of real-time collection of traffic data, or the search and seizure of stored computer data. The treaty is built around a framework of international cooperation, and establishes, as its objective, the need for the implementation of common legal procedure, with the purpose of facilitating international dealings and ensuring societal safety.

Currently, the treaty has been signed by 61 nations, 57 of which ratified their entry. Aside from the Council of Europe member states, it counts with the signature of states such as Australia, Canada, Israel, Japan, South Africa, Tonga and the United States of America. (COE, 2018)

The absence of some important members of the international community is of note. Most Asian countries have not signed the treaty, nor has the Federative Republic of Brazil, having outright refused to sign a treaty it had no part in drafting, despite having been previously described as the world hacking capital by the BBC. Also of note is the Russian Federation's refusal to sign. The only country in the COE not to be a signatory, Russia is the largest country in Europe, both in size and in population, and has suffered from a rapid increase in cybercrime in recent years. Once one takes into account the interconnectivity of the internet, it becomes increasingly important that all nations cooperate. Otherwise, the situation would allow for the existence of holes in security.

[2] Available for access at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

The INTERPOL endorsed the Budapest Convention in 2005. It is in this committee's best interests to review the terms of the agreement, as well as evaluate the efforts of all signatories and non-signatories in the defense of global network security. Delegates are encouraged to look into what the INTERPOL can do to support the treaty, both in national and international levels, seeing as this organization shares the same views on cybercrime as the convention.

4.2. Case studies

The following subsections detail select cases of notable violations in cybersecurity, and the INTERPOL's resolutions and actions in those scenarios. Delegates should study and make use of these as basis to their own resolutions.

4.2.1. Edward Snowden

Edward Snowden was born on June 21, 1983 in Elizabeth city, North Carolina, U.S. He is a computer programmer, former Central Intelligence Agency (CIA) employee and former contractor for the United States government. In 2013 Snowden collected top-secret documents regarding NSA domestic surveillance practices, copied and leaked them without authorization. After he fled to Hong Kong in June 2013 revealed thousands of confidential documents to journalists Glenn Greenwald, Laura Poitras and Ewen MacAskill, Snowden's revelations revealed numerous global surveillance programs, many administered by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunications companies and European governments. On June 21, 2013, the United States Department of Justice filed charges against Snowden for violating the 1917 Espionage Act and routing government property, shortly thereafter, the State Department revoked his passport. Two days later he flew to Moscow Sheremetyevo airport, but Russian authorities noted that his American passport had been canceled and he was stuck at the airport terminal for over a month when Russia finally granted him asylum right for a year, and repeated extensions allowed him to remain at least until 2020. In early 2016 he became the president of Freedom of the Press Foundation, an organization that aims to protect journalists from hacking and government surveillance. As of 2017 he was living in an undisclosed location in Moscow and continuing to seek asylum in other parts of the world. (NY TIMES, 2013)

The White House has rejected a petition to pardon denouncer Edward Snowden and a senior aide to Obama has said Snowden should return to the United States to face the consequences of his decision to release classified information about US intelligence gathering. INTERPOL has not released a Red Notice in Snowden's name, in keeping with the neutrality clause.

4.2.2. Julian Assange and Wikileaks:

The website Wikileaks was originally released to the public in 2006, by the Sunshine Press, as an independent non-profit media organization with the objective to spread important information and original governmental documents from anonymous sources. Originally having followed Wikipedia's model of a freely-editable website, Wikileaks currently operates in the basis of an open online space, allowing anyone to anonymously send in political, ethnical, historical documents and overall information. According to the website, the publication of this kind of material is an important tool in maintaining transparency between the people and the government. Said transparency is fundamental for the effective organization of society, being a valuable tool in the maintenance of vital democratic institutions.

Having been involved in numerous information leaks, ranging from corruption to war and torture, the organization was responsible for the leakage of the Afghanistan War Diaries, containing over 76.000 previously unreleased documents, and the Iraqi War Records, composed of a number of reports on events previously unknown or unconfirmed.

Julian Assange is an australian cyberactivist, notorious for being a part of Wikileak's council, as well as being its main public face. Less than a month after the release of the Afghanistan war documents, in the 20th of august, Assange was accused of sexual assault and rape in Sweden, and an international arrest warrant was issued, as well as an INTERPOL Red Notice. (BBC, 2010) Having turned himself over to the police in the UK, he was released on bail, which he then breached, receiving asylum and seeking refuge in the Ecuadorian embassy in London. As of 2018, the Swedish prosecutors, dropped the investigation into his rape accusations, and applied to revoke the arrest warrant, though he is still wanted for failing to turn himself in for his bail.

The allegations raised against Assange cause a fair bit of controversy, both due to their timing, a mere month after the Afghan war documents were leaked, and the United States' governmental efforts to discredit Wikileaks, divulged both by Wikileaks, in 2008 and Snowden, in 2013.

During the 2016 Democratic Party primaries, Wikileaks was involved in Clinton's email scandals, detailed below. According to some political scientists, these were released strategically in high points of Clinton's campaign, and, according to cybersecurity experts, this information was leaked to Wikileaks by Russian hackers, who had acquired the data illegally. Assange vehemently denies any cooperation with Russia in regards to these leaks, and claims Clinton was causing "hysteria about Russia".

4.2.3 Hillary's email leaks

In 2016, during the presidential campaign, famous website wikileaks released a link containing emails from both Hillary Clinton, presidential candidate, and her campaign chairman John Podesta, under the Freedom of Information Act (FOIA), an american federal law that allows the full or partial disclosure of unreleased documents controlled by the US government. The messages reveal details about Clinton's plans to garner more votes especially from left wing voters, disclosing how Hillary, along with her team, defined the political stance necessary to achieve her goal.

The leaked content, that includes more than 6 thousand emails, revealed some important information, especially about Clinton's weaknesses, notably that she has a solidified base as a politician with ties to big banks, in a time where most americans are asking for change and innovation. Some of the emails also focused on her rivals, especially candidate Bernie Sanders, her primary rival in the democratic party election, whom Podesta called a "doofus" for criticising the Paris climate change agreement. However, one of the series of leaks mentioned that the Clinton campaign wanted to be more like Sanders', that appeals to the american youth with messages of hope and change, while Clinton's was more on the negative side of the spectrum.

Another significant point leaked was that Clinton was aware of several debate questions in advance, having the time to prepare her answers thoroughly, which raised negative attention to Hillary, the public consensus being that it was unethical and she wasn't fit to be a president. Another disclosed info that helped intensify that negative reaction was that Podesta said in one of the emails that Hillary hated "everyday americans", but her campaign hinged on the basis of her "running for president because you and everyday americans need a champion".

Clinton and her party never confirmed the veracity of the emails released. But their content was still defining information during the last steps of the presidential election, because Trump's team was keen on using controversial facts disclosed, such as that Clinton supposedly received privileged information from the White House. During one of the presidential debates Trump questioned the presenter why didn't he ask about Hillary's email controversy, because he thought that the moderate party wasn't giving the due attention to the latest WikiLeaks revelations, and also to reduce the attention on himself, considering he was caught making a misogynistic comment earlier the same week.

It is appropriate to say that this scandal did have a negative impact on Clinton's votes at the end of the election, but it wasn't so substantial to the point that she lost the election because of the leaks.

4.2.4 The Deep Web’s Influence

The Deep Web, also known as Deep Net or The Invisible Web, can be understood as all the information available on the World Wide Web unreachable by the conventional search engines, such as Google and Bing. These informations are presented on pages that don't use the Domain Name System and aren't indexed with search words. Basically, it is a place remotely monitored and, therefore, provides more freedom to it's users. The lack of control over it due to the difficulty on identifying individuals is the reason that concerns authorities the most.

Interest in the Deep Web peaked in 2013 when the FBI took down the Silk Road marketplace and exposed the Internet’s notorious drug trafficking underbelly. The Dark Web wasn’t originally designed to enable anonymous criminal activities. In fact, TOR, the most popular special browsing software , was created to secure communications and escape censorship as a way to guarantee free speech. Just like any tool, its impact can change, depending on a user’s intent.

For example, it helped mobilize the Arab Spring protests. There are a lot of discussion forums and documents avaiable only on the Deep Web. In countries where censorship is significant, as China and North Korea, the anonymous web is crucial to the attempt of revealing the truth. Groups such as the aforementioned Wikileaks started on it. Around the globe, accessing the Deep Web is not a crime, but there is a huge crime web inside it.

Some cases such as the Silk Road case (USA), the Cannibal from Rothenburg (GER), the Darknet Operation (BR) and the Onymous Operation (Europe) are well know, but everyday the Deep Web is the way people all over the world use to commit crimes, from child pornography distribution to manslaughter. On April 2017, Interpol designated a task force to combat a recently discovered illegal wildlife virtual market, a slightly overlooked problem.

In the last ten years interest over safety and the Deep Web have increased. Countries all over the globe are endeavouring to develop the best way to combat the cybercrime on the Deep Web. In 2015, Interpol Global Complex for Innovation has promoted a course to representants of eleven countries to identify methods and strategies organized crime uses on the Hidden Web. On April 2018, Interpol hold the fist Darknet and Cryptocurrencies Working Group, assembling members from 18 countries. As it can be seen, the Deep Web's cybercrime has attracted the attention of the International Police and is encouraging all countries to work together against this threat.

5. Delegations and Their Foreign Policies

The United States of America

The United States of America have had a robust strategy for dealing with cybersecurity and cybercrime within the country. Through the NSA, as reported by Snowden, the USA keep a close eye in the internet dealings coming in and out of the country, as well as those within, through the lens of homeland security. The country has also adopted several governmental efforts to promote international diligence in relation to cybersecurity. The US are ratified signatories to the Council of Europe's Budapest Convention, have reached diplomatic consensus with NATO, G20, ASEAN and the OSCE in relation to establishing international courses of action to combat cybercrime, and have supported the G7's 24/7 Network (US DEPARTMENT OF STATE, 2016).

On another hand, the US have indicted 5 chinese military officers over charges of information theft. This, of course, is a symbolic act, with the indictment being highly unlikely to go through, and was paired with an addition to a "most wanted" list, along with FBI Wanted posters. The act is emblematic to the USA's policy of condemning the militarization of cyberspace, especially as it pertains to commercial benefit (NY TIMES, 2014).

Additionally, as of 2017, four of the Trump administration's cybersecurity advisors have resigned from their posts, citing lack of attention to critical issues and the delay of policy as main reasons. The administration had, in the beginning of the year, called in Rudy Giuliani to be Trump's top advisor in cybersecurity measures, due to him being a major figure in private cybersecurity. (THE WASHINGTON POST, 2017)

The United Kingdom of Great Britain and Northern Ireland

To fight cybercrime, the United Kingdom created an organ named the National Cyber Security Centre (NCSC) to provide guidance to the population in avoiding security threats, like viruses. Along with that, the government invested £1.9 billion in a cyber security strategy plan from 2016 to 2021, which aims to defend threats, deter all forms of aggression in cyberspace and develop the cyber security industry, beyond that, one of the objectives is pursuing international action, using the country's influence to invest in partnerships that guarantee the development of cyber security, that protect the UK's interests overseas. To achieve those goals, the english government will increase the number of investments, while supporting market forces to raise cyber security standards, to make possible the active application of cyber defence measures.

The Republic of India

In comparison to other more developed countries, like the USA, the concept of cybersecurity in India is quite recent. In 2013 the indian government announced new cybersecurity policy to fight NSA surveillance, and although the population was hopeful that this would be a secure method, the policy turned out to be more of a statement than a comprehensive framework for cyber security. Despite the new laws against cybercrime, hacker attacks on India are getting more sophisticated, such as, for one, a recent WannaCrypt attack that caused damage to many indian companies, affecting even the government.

The Russian Federation

When it comes to cybersecurity, Russia is quite a controversial country, since the USA accused Russia of a cyber attack on the energy sector, and russian hackers perform such a powerful cyber attack on Germany that it was called a "form of warfare". Despite those controversies, the russian government worries about the cybersecurity of its inhabitants, so they issued a cybersecurity strategy to 2020 in 2009, which provoked a varied response, since the population did not think that it was an effective enough policy to stop cyberattacks in the country.

The Federal Republic of Germany

The government of Germany, on September 20, 2006, proposed a new bill on cybercrime. these laws are designed to end any gap in previous constitution. The current Penal Code guarantees that any person convicted of spying or altering data or sabotage by computer shall be punished with imprisonment and payment of fines.

The Germany’s army are one of the world's top spy targets, not just because of the military secrets, but also because of its weapons systems supported in Information Technology. in December 2016, Germany's domestic and foreign intelligence agencies reported the rise of Russian cyber-attacks against political parties (although Russians deny espionage). For these reasons in 2017, the German defense minister created a new command unit (Cyber and Information Space Command). The base of the new German command is Bonn, with an initial team of 260 people (REUTERS, 2017)

The Federative Republic of Brazil

In April 2, 2013, anti-cyber crime laws in Brazil came into force after President Dilma Rousseff signed in December 2012. The law classifies various crimes involving stored personal information, invasion of third-party electronic systems, and production of programs that allow the invasion of systems

and computers. The bill was initiated after an incident in May 2012, in which Brazilian actress Carolina Dieckmann was blackmailed. Prior to this law, the cybercrimes committed in Brazil were not defined as criminal offences but treated as if they were a violation of communication.

As of 2017, Brazil is one of the countries that registered the most cybercrime activities in the world, being in fourth place. The survey also revealed that more than 42 million people were affected by cybercrime. (NORTON, 2017)

The French Republic

The eve of the French presidential election of 2017 was marked by the repercussion of a cyber attack against the candidate Emmanuel Macron. Several documents were leaked by an anonymous source. the document contained false information mixed with the truth about his team. After this cyber attack against Macron, France reinforced security. (REUTERS, 2017)

Data protection laws in France are generally ahead of the international curve. In addition to being bound by the new European General Data Protection Regulation, which was adopted by the European Parliament on 27 April 2016 and will come into force from 25 May 2018.

Japan

Ratified signatory to the Council of Europe's Budapest Convention, Japan initiated a intense combat against the cybercrime in the 2010 decade. From an attempt to block the use of TOR inside your boundaries (BRITISH BROADCASTING CORPORATION, 2013) to the creation of a Metropolitan Police Department division specialized in cybercrime (REUTERS JAPAN, 2017), the enormous teconopole is investing a lot of its technological resources to guarantee the virtual security.

People's Republic of China

Seeking a competitive superiority, China have been developing a strong IT education among the new generations. Although it is positive in many ways, it made China the country number one in cybercrime activity (CYWARE, 2017).

The securitie strategies adopted by the government are,sometimes, quite controversial. Creating a cybercrime specialized division, responsible for thousands of arrests in just a semester (PEOPLE'S REPUBLIC OF CHINA EMBASSY, ,2015), establishing in 2016, by law, that every big company on the

country can be subjected to a government security review and even using the Internet Censorship Law to block the access to malicious virtual pages are some examples.

Republic of Turkey

With a Department for Cyber Crimes, Turkey has an extense legislation against virtual transgressions created from the Budapest Convention. According to the Turkey National Police, training modules on cybercrime investigations and electronic evidence were devised and offered to prosecutors, judges and law enforcement officers and, in order to facilitate immediate assistance in international cybercrime cases, point of contact staff were designated and trained to be available on a 24 hour, 7-day-a-week basis (Delegation of the European Union to Turkey).

It is relevant that in the global cyber attack traffic, Turkey takes a share of 4.7%. Turkish hackers have increased their activities in the last decade, and in the cybercrime ranking, the third place is taken by Turkey (CYWARE, 2017).

6. Points of discussion

The INTERPOL is an international body, responsible for enabling the coordination of police forces around the globe. Therefore, delegates are encouraged to look at these questions to guide their discussions:

- How can the INTERPOL help evaluate the efforts of the Budapest Convention's signatories, and how can it evaluate criticisms to the treaty itself?
- How can the INTERPOL help make the Budapest Convention more viable? Can the organization help bring more signatories to the treaty?
- How can the organization achieve collaboration with their criminal databases after recent espionage scandals like the Snowden case?
- Should Article 3 of the organization's constitution be reevaluated? Is acting upon political crimes adequate within INTERPOL's scope?
- What should the organization's stance be in regards to the Deep Web?

7. References

BRITISH BROADCASTING CORPORATION. **Japanese police target users of Tor anonymous network.** Available in: <http://www.bbc.com/news/technology-22248692> Accessed in May 1st, 2018

BRITISH BROADCASTING CORPORATION. **Interpol issues 'Red Notice' for Wikileaks' Assange.** Available in: <http://www.bbc.com/news/world-europe-11883567> Accessed in April 15th, 2018

CHINA EMBASSY. **Polícia da internet da China fortalecerá combate aos ciberdelito**. Available in: <http://br.china-embassy.org/por/szxw/t1269128.htm > Accessed in May 6th, 2018

CIÊNCIAS CRIMINAIS. **Deep Web: o submundo do crime**. Available in: <https://canalcienciascriminais.com.br/deep-web-o-submundo-do-crime/ > Accessed in April 20th, 2018

CIÊNCIAS CRIMINAIS. **Ainda sobre a Deep Web: o lado positivo da rede**. Available in: <https://canalcienciascriminais.com.br/ainda-sobre-a-deep-web-o-lado-positivo-da-rede/ > Accessed in April 20th, 2018

CIÊNCIAS CRIMINAIS. **Aquém da superfície: verdades e mitos sobre a Deep Web**. Available in: <https://canalcienciascriminais.com.br/aquem-da-superficie-verdades-e-mitos-da-deep-web/ > Accessed in April 20th, 2018

COMPUTERWORLD. **China apresenta nova lei de cibersegurança e preocupa empresas de TI.** Available in: <http://computerworld.com.br/china-apresenta-nova-lei-de-ciberseguranca-e-preocupa-empresas-de-ti > Accessed in May 4th, 2018

COUNCIL OF EUROPE. **Convention on Cybercrime**, Budapest, 2001. Available in: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> Accessed in April 4th, 2018

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 185 (Convention on Cybercrime).** Available in: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures> Accessed in April 28th, 2018

COUNCIL OF EUROPE. **Turkey Status regarding Budapest Convention**. Available in: <https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/turkey/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=en_GB > Accessed in May 5th, 2018

CYWARE. **Top ten countries with most hackers in the world.** Available in: <https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94 e> Accessed in May 4th, 2018

DELEGATION OF THE EUROPEAN UNION TO TURKEY . **Combating cybercrime.** Available in: <https://www.avrupa.info.tr/en/combating-cybercrime-164 > Accessed in May 4th, 2018

ESTADO DE MINAS . **Polícia encerra atividade de mercados da 'deep web'.** Available in: <https://www.em.com.br/app/noticia/internacional/2017/07/20/interna_internacional,885382/policia-encerra-atividades-de-mercados-da-deep-web.shtml > Accessed in April 20th, 2018

FOLHA DE SÃO PAULO . **Interpol cria sua própria 'dark web' para estudar crimes virtuais .** Available in: <http://www1.folha.uol.com.br/tec/2015/08/1670190-interpol-cria-sua-propria-dark-web-para-estudar-crimes-virtuais.shtml?loggedpaywall > Accessed in April 20th, 2018

GERCKE, M. **Understanding cybercrime: phenomena, challenges and legal responses.** ITU. Geneve, Switzerland, 2012.

INTERPOL. **Cybercrime.** Available in: <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> Accessed in April 4th, 2018

INTERPOL. **The Constitution.** Available in <https://www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution> Accessed in April 4th, 2018.

INTERPOL. **INTERPOL Darknet training shines light on underground criminal activities.** Available in <https://www.interpol.int/News-and-media/News/2015/N2015-108 > Accessed in April 22nd, 2018.

NORTON. **Norton Cybersecurity Insights**. Available in <https://us.norton.com/cyber-security-insights-2017> Accessed in April 28th, 2018

NEXO. **O que é a deep web e por que ela está encolhendo.**Available in <https://www.nexojornal.com.br/expresso/2017/03/17/O-que-%C3%A9-a-deep-web-e-por-que-ela-est%C3%A1-encolhendo > Accessed in April 24th, 2018

PHYS. **Using science to combat illegal wildlife trade**. Available in <https://phys.org/news/2017-07-science-combat-illegal-wildlife.html > Accessed in April 21st, 2018

REUTERS. **German military to unveil new cyber command as threats grow.** Available in <https://www.reuters.com/article/us-germany-military-cyber/german-military-to-unveil-new-cyber-command-as-threats-grow-idUSKBN1712MW> Accessed in April 28th, 2018

REUTERS. **Macron campaign was target of cyber attacks by spy-linked group.** Available in <https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200> Accessed in April 15th, 2018

SOPHOS. **China promete limpar internet do cibercrime.** Available in: <https://nakedsecurity.sophos.com/pt/2015/08/20/china-vows-to-clean-the-internet-in-cybercrime-crackdown-15000-arrested/ > Accessed in May 6th, 2018

THE NEW YORK TIMES. **5 in China army face US charges of Cyberattack.** Available in: <https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html> Accessed in April 28th, 2018

THE NEW YORK TIMES. **Snowden, in Russia, seeks asylum in Ecuador.** Available in: <https://www.nytimes.com/2013/06/24/world/asia/nsa-leaker-leaves-hong-kong-local-officials-say.html> Accessed in April 15th, 2018

THE WASHINGTON POST. **Trump names Rudy Giuliani as cybersecurity advisor.** Available in: <https://www.washingtonpost.com/news/powerpost/wp/2017/01/12/trump-names-rudy-giuliani-as-cybersecurity-adviser/?utm_term=.4ea23e84ff7a> Accessed in May 5th, 2018

TREND MICRO. **Below the surface: exploring the deep web.** Available in: <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf > Accessed in April 20th, 2018

US DEPARTMENT OF STATE. **International Cyberspace Policy Strategy.** Available in: <https://www.state.gov/documents/organization/255732.pdf> Accessed in April 28th, 2018

8. Appendix:

8.1. On the Topic of Notices and Resolutions

This committee is **not mandatory**, and, therefore, its resolutions are not binding. It is, however, the organization's mission to make recommendations and develop databases and framework to facilitate police work around the globe.

Resolutions are to be drafted following the UN model standard, requiring at least 6 preambulatory clauses, followed by the required number of operative clauses. It requites a minimum of 4 signatories to be presented to the committee. Models for the standard INTERPOL resolution are available through the organization's website[3]. Any notices presented by the committee will be archived and later put to a separate vote, to take place after the approval of the final Draft Resolution.

8.2. Glossary

Points

-*Point of Inquiry*: Meant for questions regarding the flow of the debate and the procedures and rules of the committee;

-*Point of Order*: Meant to point out any mistake the members of the chair may have committed;

-*Point of Personal Privilege*: Meant for PERSONAL matters only. Meant for use if anything is bothering you personally, be it an insult to you, or a discomfort caused by heat or lack thereof.

Motions

There are many motions a delegate may ask that change the flow of the debate. They are, in order of precedence:;

-*Motion for adjournment of the session*: Dismisses the committee until the next session. Requires qualified majority.;

-*Motion for extension of moderated/unmoderated caucus*: Each caucus can be extended only once, it needs to have the same purpose, time limit and time of speech of the original caucus. Requires simple majority;

-*Motion for unmoderated caucus*: Changes the flow of the debate. During an unmoderated caucus, the chair doesn't interfere with the debate, delegates may get up from their desks and talk at any time. Delegates must specify time limit and purpose. Requires simple majority;

3 https://www.interpol.int/About-INTERPOL/Structure-and-governance/General-Assembly

-*Motion for moderated caucus*: Changes the flow of the debate. During the moderated caucus, every delegation raises their plackards and the chair decides who gets to speak, between those who asked to do so. Delegates must specify time limit, time of speech and purpose. Requires simple majority;

-*Motion for changing the time of speech*: Changes the time of each speech. Delegates must specify a reason. Requires simple majority.;

-*Motion for closure of the debate*: Closes the debate on specific substantive matters. If it passes, the committee proceeds to vote the matter. Requires qualified majority;

-*Motion for closure of the speaker's list*: Can only be used in the Special Speaker's list, such as the one used for debating draft resolutions. Prevents any delegations from entering their names on the list. Requires qualified majority;

-*Motion for reopening of the speakers list*: Reopens the speakers list, it it's closed. Requires qualified majority;

-*Motion for introduction of Draft Resolution/Notice*: Must be approved by the chair. Introduces the Draft Resolution, which must have already been appraised by the chair. Automatically opens a special speakers list for debating the draft resolution;

-*Motion for introduction of Amendment*: The same as the introduction of draft resolution;

-*Motion for introduction of a working paper*: Introduces a working paper for the committee;

-*Motion for Roll Call Voting*: In order only for substantive matters, changes the form of voting.