ISTMUN

SECURITY COUNCIL

CYBERCRIME AND IT´S THREAT TO NATIONAL SECURITY

WELCOMING LETTER

Dear delegates,

It is our pleasure to be directing this committee in this limited edition of the Model of United Nations, currently we are both coursing eleven grade in Aspaen Gimnasio Iragua and San Tarsicio school respectively. It is an honour for us to be leading the Security Council and our intention is that every delegate achieves and fulfills their own expectations. We consider participating in Models of the United Nations a very enriching activity, due to the fact that very delegate has the opportunity to develop negotiating, speaking, investigative and debating skills. As the chair, we hope you find this document useful for your preparation in order to achieve a challenging and dynamic debate, with creative but realistic solutions; keep in mind that a wider research is expected in order to contribute to the discussion with relevant and substantiated arguments.

ISTMUN is a learning space where participants will be able to develop their abilities as well as encounter new ones working towards the development in your own academic field and nurturing your acts of progress towards society. We invite you to take advantage of this experience demonstrating your leadership, communication and peacemaking abilities that put together a committed delegate and citizen.

During the committees sessions, let us know any questions you have. Meanwhile, don't hesitate to e-mail us for any doubt you might have, we are glad to help you make the best of this committee.

Sincerely,
Security Council of the United Nations' chair.

Camila Rozo
Aspaen Gimnasio Iragua
mcamilarozogarcia@gmail.com

Antonio Gallego
Colegio San Tarcisio
antonio.gallego.ortiz@gmail.com

INTRODUCTION TO THE COMMITTEE

Along with the expected, argumented and substantiated research, delegates should hand in a well structured position paper and an opening speech as well as complete knowledge regarding procedure held on the handbook.

Position paper

A position paper is an overview of the countries' posture regarding the topic that is being held, which should be structured around framing what the country thinks about the problem, how is it involved in the situation and what proposals or likely solutions could be implemented. The document should be written in Arial 12 with 1.0 space line, and an approximate length of 1 or 2 pages. The first paragraph should present an introduction with accurate facts of the countries' position. The second paragraph should specify the already developed aspects and programmes regarding the topic and how your nation collaborated with them, alongside with previous resolutions, laws, and official declarations. Lastly, the third paragraph should include the conclusions, your proposals and the way you plan to implement them within the committee. Please deliver your position paper to the mentioned mails on the 12 of February and bring it printed on the 15th of February.

Opening speech

An opening speech is a diplomatic document meant to be read at the beginning of the first session, in order to provide a general view of the position of your country regarding the topic on debate. The document should have a header that includes the name of the committee, the name of the country, and the topic. The first paragraph shall consist of the greetings; the second paragraph should introduce the posture of your country concerning the topic; the third paragraph should present the position of your delegation with facts and specific data, along with the achievements done by the country; finally, in the fourth paragraph, you shouldinclude the conclusion of the speech. If you wish, you can close your speech with a quote. It must have a length of 1 minute per speaker.

BACKGROUND

The United Nations Security Council is one of the five main organs of the United Nations, alongside with the General Assembly, the Economic and Social Council, the International Court of Justice and the Secretariat. It is composed by 15 members, of whom five of them are permanent and have the veto power: the French Republic, the People's Republic of China, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland and the United States of America. The other ten members are non-permanent, which are elected every two years by the General Assembly. The article 27 of the UN Charter settles voting as a mandatory procedure, therefore, every decision made by the Council will pass under the vote of 9 members, including the vote of each veto power.

According to the UN Charter, the Security Council has four main purposes: to maintain international peace and security, to develop friendly relations among nations, to cooperate in solving international problems and in promoting respect for human rights; and to be a center for harmonizing the actions of nations. Article 39 of the United Nations Charter states that the Security Council shall determine the existence of any threat to the peace or act of aggression; consequently, the organ is responsible of acting as a mediator between the actors in conflict by trying to reach agreement by peaceful means. When a dispute leads to hostilities, the Council's primary concern is to reach a ceasefire.

As stated by the official website of the United Nations Security Council, it's main functions and powers are:

- To maintain international peace and security in accordance with the principles and purposes of the United Nations;
- To investigate any dispute or situation which might lead to international friction;
- To recommend methods of adjusting such disputes or the terms of settlement;
- To formulate plans for the establishment of a system to regulate armaments;

BACKGROUND

- To determine the existence of a threat to the peace or act of aggression and to recommend what action should be taken;
- To call on Members to apply economic sanctions and other measures not involving the use of force to prevent or stop aggression;
- To take military action against an aggressor;
- To recommend the admission of new Members;
- To exercise the trusteeship functions of the United Nations in "strategic areas";
- To recommend to the General Assembly the appointment of the Secretary-General and, together with the Assembly, to elect the Judges of the International Court of Justice.

Article 25 of the UN Chart establishes that all the members of the UN agree to accept and carry the decisions of the Security Council. While other organs of the United Nations make recommendations to member states, the Security Council has the power to act and make decisions that all the member states of the United Nations must implement.

Committee's history

For preventing another worldwide catastrophe after World War II, a comprehensive determination of creating a new organization which would ensure international peace, cooperation and security between nations emerged. In 1944, during the Dumbarton Oaks conference held in Washington D.C., several nations planned proposals that became the basis for the United Nations. Hoping that the organization's creation would represent an effective answer to potential global disputes to any threats to peace, the composition of the Security Council became a prevalent concern. In 1945, representatives from 50 countries met in San Francisco to draw up the United Nations Charter, which was signed on June 26 of the same year. Since then, the United Nations was definitely established, and, through its main six organs, it has committed to guarantee the maintenance of peace and international security to this day.

During the Cold War, the Security Council was directly affected due to the repetitive usage of the veto power from the permanent members, especially

BACKGROUND

the United States of America and the Union of Soviet Socialist Republics (nowadays the Russian Federation). As a result, the organ was criticized for the way decisions had been taken. After the Cold War, the Council had more opportunities to act under the principles with which it was created.

.

CYBERCRIME

TOPIC: Cybercrime and its threat to National Security

What is cybercrime?

In today's society information management as well as global communication are done in a much more effective and faster way than ever before because of how highly reliant mankind is on modern technology. Nevertheless, as much advantages as it brings, risk of theft, fraud and abuse is as well increased. (Homeland Security, n.d.). Cybercrime is a fast-growing criminal form because of its convenient speed, anonymity and extension of possible action. (INTERPOL, n.d.)

Even though there is not a specific worldwide accepted definition for cyber crime, over the last decades and the rapid evolution of technology, cybercrime has been an arising topic. After the creation of the Convention on Cybercrime of Council of Europe, a broader concept from a global angle was formed, defined in five dimensions which follow: "(i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) Computer related offences; (iii) content related offences; (iv) offences related to infringements of copyright; (v) abetting or aiding such offences" (Halder, 2012, p. 13). Crimes are usually classified into two categories by law enforcement; on one hand, advanced cybercrime, typically defines high technology crimes where sophisticated methods are carried away to attack any kind of hardware or software. On the other hand, cyber-enabled crime refers to the more common and traditional modalities which make use of the internet and technological means to execute any kind of crime predominantly financial crimes, crimes against children and terrorism. (INTERPOL, n.d.)

Regarding cybersecurity and law enforcement

The implementation of cybersecurity parameters into law enforcement is generally considered necessary to safeguard the cyberspace and prevent criminal activity in order to maintain not only national but international security as one of the main objectives that the committee has. Nevertheless, as of today, state responses towards the establishment of regulated law enforcement mechanisms have not been able to keep up with the rapid evolution of cyberspace (Tabansky, 2012).

CYBERCRIME

Given that carrying out cybercrimes have a substantially lower physical risk as well as identity discovery, the risk of punishment is, in like manner, decreased, owing to how cyber crimes are generally perceived as non-violent with less harmful extension ergo, it is treated accordingly.
It is of great importance to develop a broader understanding of the implications in order to develop suitable mechanisms with global extent; likewise, the “sovereign enforcement bodies operating on the basis of national legal infrastructures” (Tabansky, 2012, p. 118) should earmark specific resources to the creation of precautionary, investigative and punitive mechanisms for crimes related to the cyberspace. Treaties and actions with worldwide impact such as the European Council’s Budapest Convention on Cybercrime, several resolutions and conferences held by the United Nations, the Organisation for Economic Co-operation and Development (OECD), the European Union and the International Telecom Union. However, the state is the sole responsible for the maintenance of its citizens security and international treaties cannot replace sovereign policy of independent states.

Cybercrime and National Security

The implications of cyber crime towards national security include the efficient access with such speed, immediacy, remote operation, encryption and obfuscation that high technology and computerization allows; which hinders the identification of the operation and the operator. Tasks can be broken down into small units, therefore process are decentralized. Networking allows global access to information and focus on knowledge as a valuable product, therefore, it is prone to be attained, disrupted and manipulated for gain. (Tabansky, 2012)
Given the severity of the crime, and whether it involves the integrity of a computer system referred as hacking, the one developed in cyberspace such as encrypted communications among individuals on the fringes of the law or any crime involving computerized information contents where theft of secrets, dissemination of harmful contents are managed, it still signifies a threat and risk to national security and easier access to international territory when identity is hidden and resources decentralized.

CYBERCRIME

Cybercrime affects security in a variety of ways. For example, a malicious actor who gains unauthorised access to secret commercial information could, therefore, exploit vulnerabilities in an entity's or individual's computer system, cyber-attacks on telecommunications systems that affect lines of communication across sea and air routes could inhibit crucial actions such as international trade and access to externally sourced resources; likewise, technologically advanced computer tools are prone to be used to target several institutions such as the defence forces information networks where substantial information could be exposed including ballistic missile defence systems or communications satellites being cybercrime a growing issue that challenges every nation worldwide.

As an evolving transnational crime, it's complex nature is rapidly changing and efficiently developed given the border-less realm of cyberspace among with the increasing involvement of organized crime groups. Perpetrators of cybercrime as well as their victims can be located in a wide range of regions which implies difficulties when fighting against it. Moreover, its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic and international response. As members of the Security Council, it is of great importance that the discussion is guided towards the examination of options that may strengthen existing strategies and the proposal of new national and international legal or other responses to cybercrime. (UNODC, n.d.)

While there is no specific Sustainable Development Goal that tackles cyber crime specifically, it is a direct an indirect burden to a number of objectives such as matters regarding the goal 16 related to violence and crime which include corruption, arm trafficking and more. It is pivotal to control such expanding crime form to achieve the sustainability needed to safeguard peace. Furthermore, the scope of what illicit activity through cyberspace can reach opens several more threats that extrapolate the virtual field. The use of technology or cyber-enabled and cyber-dependent activities can facilitate a span of activities such as the recruitment of trafficking victims, sexual exploitation or the dissemination of offensive and problem-seeking information.

CYBERCRIME

Global context

Each year, Europol's European Cybercrime Centre publishes the Internet Organized Crime Threat Assessment (IOCTA), which is an strategic report on key findings and emerging threats and developments in cybercrime, and it is based on the Internet Security Threat Report (ISTR) done by Symantec, an international corporation, global leader in cyber security, identified the geographic distribution of cybercrime as the following:

- North America
North America, particularly the USA, continue to be both a key originator and a target of global cyber-attacks domestically and from overseas. Various reports have indicated that North America is a primary target for global ransomware attacks (form of malicious software, that deletes and corrupts files for the purpose of looking for a monetary compensation), and mobile malware. Moreover, the APWG identifies both USA and Canada as top countries for the hosting of phishing sites (websites that attempt on stealing confidential information). (Europol), (2018)

- Latin America
Latin America also features heavily in cyber security reporting. Lack of adequate cybercrime legislation has resulted in Brazil being both the number-one target and the leading source of online attacks in Latin America. Similar to the USA, Brazil is also a top host of phishing sites, with some reporting putting Brazil as one of the world's top ten originators of all cyber- attacks. The profile of Mexico is becoming increasingly prominent, with Mexico suffering from the largest number of cyber- attacks in Latin America after Brazil. (Symantec), (2018)
The primary threat coming from the Americas as a whole, from a law enforcement perspective, associates to various aspects of payment fraud.

- Europe
The majority of cyber threats affecting Europe continue to emanate from within the same continent. Austria, Germany, Hungary, Italy, Russia, Spain and the UK, had some of the highest global rates of malicious emails containing malware, and Ireland, Norway and Sweden similarly had some of the highest global rates of

email containing malicious URLs. Moreover, the Netherlands, Hungary, Portugal and Austria, also suffered from high global rates of phishing emails. Moreover, some EU countries, such as France and Germany are significant global sources of spam.
Law enforcement outlined a wide variety of cyber-attacks emanating from other European countries, although there was strong emphasis on various aspects of payment fraud. In this regard, Bulgaria and Romania were highlighted as having a key role. (Europol), (2018)

- The Middle East and Asia

A 2017 report by Trend Micro details a burgeoning digital underground active in the Middle East and North Africa. The report highlights that while the scale and scope of products and services does not compare to more mature markets, a wide variety of malware, crime tools and weapons is still available on these markets. Such markets are however, heavily influenced by culture and ideology and consequently operate very differently to the criminal markets European investigators may be familiar with. It is common practice to share code, malware, or instruction manuals for free in a 'spirit of sharing'. The main cyber activity carried out on these context, is hacktivism and largely limited to website defacement and DDoS attacks (Distributed denial of service, which is an attack to a system of computers or network that causes a service or a resource, to be inaccessible to legitimate users). However, it is anticipated that these markets will evolve and mature into more serious attacks, particularly given the already visible influence of the Russian underground. (Symantec), (2018)

- Asia

Based on industry reporting, cyber-attacks directed towards Asia countries appear to follow a different profile and methodology compared to those commonly encountered in Europe. While emails loaded with malicious attachments are still noted in several south-east Asian countries, like Malaysia, Kuwait and Taiwan, the use of malicious URLs to the same effect appears to be very limited. However, higher rates of phishing, particularly again in Southeast Asia, suggests that compromised credentials are still highly valued. China also has one of the world's

highest rates of spam. Asia also appears to be one of the primary regions subjected to targeted cyber-attacks. While the US was top for such attacks, seven Asian countries featured within the top ten. Asia is one of the regions particularly plagued by mobile malware. China is also consistently the home of the highest number of botnet-forming IoT (Internet of Things) devices, by some margin. (Europol), (2018)

- Oceania

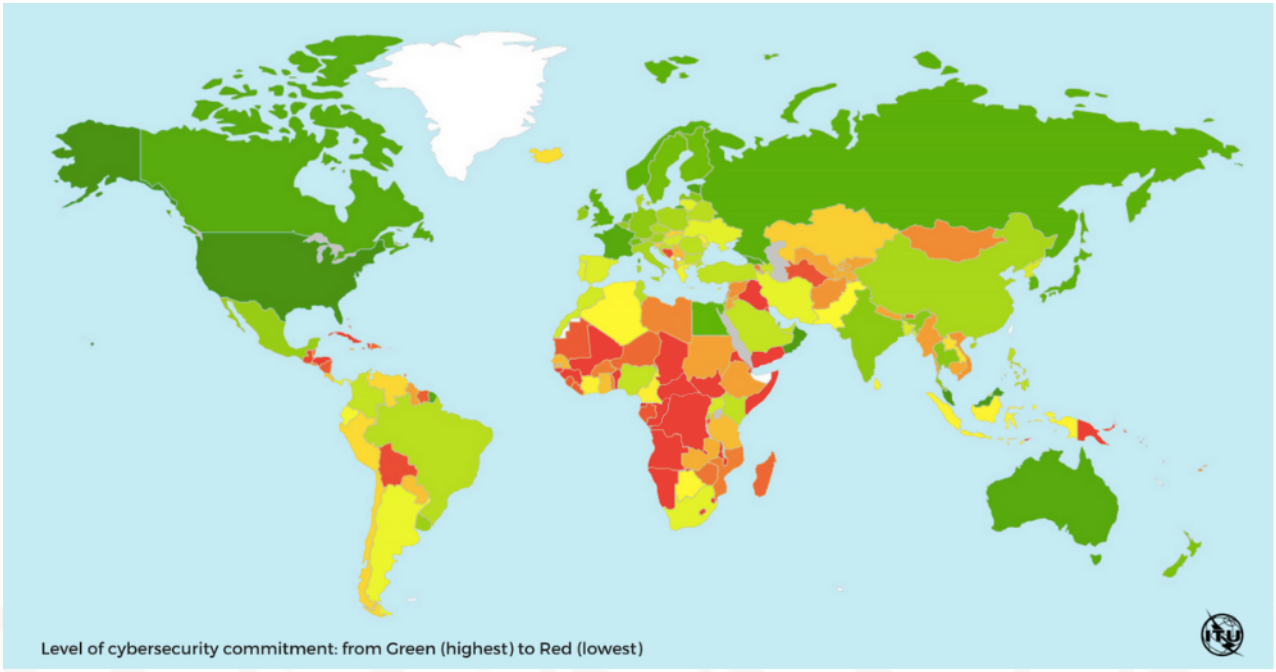
The major cyber-threats reported by the Australian Cyber Security Center (ASCS) are ransomware, data stealing malware (including the mobile variety), social engineering, Distributed Denial of Services, supply chain attacks and growing levels of state- sponsored activity. Australia and New Zealand both are recipients of significant proportions of emails containing malicious URLs. (Symantec), (2018)

Cybersecurity Index

As well as cybercrime, measuring commitment regarding cyber security and its awareness should as well be globally accessed in order to lay out the effective and coherent mechanisms that lack towards law enforcement; its strengths and weaknesses. Therefore, it is of great importance to take into account The Global Cybersecurity Index (GCI) regarding the “legal, technical, organizational, capacity building and cooperation” (Sanou, 2017, p. 2) implications.

As a consequence of the growing influence of ICT’s around the globe and their usage, a direct correlation can be found with their illicit and malicious use. To counter this effect, cybersecurity is becoming more and more relevant as an international discussion.

CYBERCRIME



Heat Map of National Cybersecurity Commitments

The Heat Map lays out a visual overview regarding the place of commitment in which every country stands regarding cybersecurity; the green ones refer to the highest and red the lowest. When analyzing the trends it is clearly seen that continents such as Europe and North America have a strong commitment. On the contrary, South America and Africa on a higher scale, showcase poor or nonexistent management towards law enforcement through cyberspace. However, taking into account that every continent has a minimum of two states with leading nations in the topic allowing to conclude that high commitment in cybercrime legislation is not strictly and specifically tied with geographic location. However, it is of great importance to take into account the different implications that could affect the rise of cybercrime and its corresponding law enforcement.

QARMAS

- Is it necessary to establish a worldwide definition of cyber crime?
- Should a general legislation be applied to all the members?
. Is law enforcement regarding cybercrime effective in your country?
- Is cybercrime a matter of national security?
- Regarding belligerent non-governmental groups that use internet for commiting crimes that affect national security, how should the Security Council act to confront the issue, and how nations should manage it?
- How can governments manage the role and participation of specialized professionals (hackers) that can be part of belligerent non-governmental groups that can produce cyberattacks?
- Should there be a monitoring system applied in order to manage future attacks? How can it be implemented?
- Which should be the criteria for future partnerships with International Organizations to confront cyber crime alongside with the security council and member nations of the United Nations? If so, how can the Security Council work along with these organizations?
- Should the Security Council impose conditions to ensure that cyber criminals do not attack?
- What are the mechanisms each government should adopt in order to prevent cyber attacks from happening, or happening less frequently?
- How should hackers be judged in case of committing a cyber crime?

Context Paragraph

The Security Council will be managed as an open agenda committee, meaning that the topics treated throughout the sessions will revolve around specific crisis and worldwide problematics regarding the jurisdiction and purpose of the before mentioned; likewise, the World Leader Summit committee will function along with the Security Council, that is, that what happens in one will have a repercussion in the other, simulating a real world situation where coherence and teamwork is especially needed.

Moreover, the committee's discussion will orbit around a core topic related to Cybercrime and its threat to national security. Subtopics such as current legislation, potential threats, weaknesses around law enforcement frameworks and the role that the Security council as a United Nations committee should play in order to appease and avoid a latent conflict. Similarly, it is of great importance to outline a definition and explore the relation between

BIBLIOGRAPHY

Tabansky, L. (2012, December). Cybercrime: A National Security Issue? Military Ans Strategic Affairs, 4.

Halder, D., & Jaishankar, K. (n.d.). Cybercrime and the Victimization of Women; Laws, Rights and Regulations (Vol. 1). United States: IGI Global
Interpol. (n.d.). Cybercrime. Retrieved from https://www.interpol.int/ Crime-areas/Cybercrime/Cybercrime

Gybson, N. (2018, March 23). Why is Cyber Crime a national security concern? Lexology.trieved from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Sanou, B. (2017). Global Cybersecurity Index 2017 (Publication). International Telecommunication Union (ITU).

Malby, S., Mace, R., & Holterhof, A. (2013, February). Comprehensive Study on Cybercrime [Draft]. Retrieved from https://www.unodc.org/documents/ organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Symantec. (2018). Internet Security Threat Report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
Europol. (2018). INTERNET ORGANISED CRIME THREAT ASSESSMENT. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/ internet-organised-crime-threat-assessment

UNDOC. (2017). Global Programme on Cybercrime. Retrieved from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
European Union Agency for Network and Information Security. (2016). Nation Cyber Security Strategies. Retrieved from https://www.enisa.europa.eu/topics/ national-cyber-security-strategies/ncss-map

BIBLIOGRAPHY

Europol. (2017). Cybercryme trends in Europe. Retrieved from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime?ct[article]=article&ct[event]=event&ct[guide]=guide&ct[panel]=panel&ct[multimedia]=multimedia&ct[news]=news&ct[operation]=operation&ct[page]=page&ct[document]=document&page=1

Europol. (2017). European Cybercrime Centre - EC3. Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Symantec. (2016). CYBER CRIME & CYBER SECURITY TRENDS IN AFRICA. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/cyber-security-trends-report-africa-interactive-en.pdf