THE VICTORIA SCHOOL
MODEL OF UNITED NATIONS XIV

GAC

Deputy Gabinet of Crisis

Presidents:

Ban 1:

Pablo Martinez- Gimnasio Moderno
pablomc@gmoderno.co
+57 3164463905

Sebastian Quiroga - The English School
sebastianquiroga@englishschool.edu.co
+57 3057845604

Ban 2:

Sofia Santamaria- Amadeus International School
sofiasantamaria2003@gmail.com
+57 3168797450

Alejandro Vega- Universidad del Rosario
alejandro.vegab@urosario.edu.co
+57 3186965270

Strategy Center:

Valentina Herrera- SC director
valentinaherreravelasquez@gmail.com
+57 3133578255

Natalia Rodriguez- Colegio la Enseñanza
natalia.rodriguez@ebog.edu.co
+57 3212721648

Mateo Illidge- Universidad Militar
mateoillidge@gmail.com
+57 3114861861

Samuel Barrera- Colegio San Carlos
samuelbalo88@gmail.com
+57 3102856810

Level of the committee: Senior

Language: English

Topic:

- Revealing secrets from the screen, International Cybercrime

Welcome letter to GAC:

Dear Delegates,

It's our pleasure to welcome you to the fourteenth edition of The Victoria School Model United Nations and it's our delight to be your presidents in this Crisis Cabinet. As your presidents, we would like to share with you our passion and dedication for this academic exercise that has allowed us to recognize diverse situations around the world and exhorts us to participate in the diverse realities different nations face in global contexts. At TVSMUN, you will have the opportunity to develop fundamental skills for life and thus achieve what we have called "Connecting Realities".

In this occasion the Crisis Cabinet will require great skills in identification and solution of problems. Also, respect and dialogue will be essential for the development of this commission. Let us remember that according to the Latin phrase "Per ardua Ad Astra" through what we consider difficult, arduous, we can finally see the stars. What involves effort has its virtue. "The study has its bitter roots, but the fruits are sweet." We invite you to fill yourself with knowledge during the days of the model in which you will have the unique opportunity to represent a delegation in an exemplary way along with its ideals in the most appropriate way.

Sincerely,

Pablo, Sofía, Sebastián & Alejandro.

About GAC

Crisis Cabinets are committees that usually recreate conflicts or historical milestones through the interaction of two factions representing the parties involved in the conflict, this being through the Strategy Center; An impartial entity that defines which of the actions proposed by each side will be taken into account for the development of the conflict in addition to what will be the repercussions of the same as well as the conclusion of the confrontation.

Crisis Cabinets are committees that reward creativity and quick action to the continuous crises to which delegates will be exposed, considering the argumentation and ideology of each of the pertinent characters, following the common thread of the theme and the current situation that they formulate.

For a correct development of the committee, for the Chair it is pertinent to take into account the following factors that intervene in it as part of the procedure:

1. Generate initiative in the immediate resolution of each crisis, leaving a record respectively through the directives.
2. Awareness about the time-space variable will be of the utmost importance, since it is the starting point for the generation and ramification of all the arguments presented during the debate sessions in order to make the intention and orientation much more truthful and accurate. of the side
3. Encouraging the notification of any doubt in front of the table is the pillar for the joint construction on each side of a comprehensive process for the GAC.

General specifications

For the purposes of this text, it is clarified to the reader that this academic guide will serve as a preparation and contextualization tool regarding the concept of international cybercrime. Within this document, the characteristics of international cybercrime, its possible origin, its particularities and its prosecution (at a general level) will be presented. **The context and the**

scenario in which the committee will be developed will be given on the first day of the model through an initial crisis statement.

Revealing secrets from the screen, International Cybercrime

Introduction

Technology has changed the way people interconnect around the globe. The flagship of globalization is the Internet. Nevertheless, as the tools used to interconnect the world before, the Internet can become a weapon in the eyes of states and criminals alike. Known as cyberwarfare, these attempts to throw into disorder information technology systems have caused a desperate discussion on how countries have to respond to these growing menace.

As the international community struggles to protect their networks and linked infrastructure from cybernetic threats, security against foreign-based attacks has become a sustancial matter in the discussion related to global security. Countries are concerned about the potential cybernetic attacks have to threaten and affect their citizens , corporations, states, societies and regional systems. The anonymity of attacks is the greatest part of the issue; attackers can easily affect individuals, attack government agencies and private corporations without revealing their identity. Given the international nature of most of these attacks, international organizations like the United Nations have been pressured to address the rise of international cybercrime and the security measures against them with the objective of promoting new international regulations regarding cybersecurity.

Broadly, the international organisms have faced a major roadblock related to cybercrime. Countries have different positions on whether international organisms should have oversight over what a nation does in cyberspace. Some of them, insist current international laws can sufficiently deal with cyber threats. Others fear expanding international law will be used to narrow their national power on the matter, or might undermine their freedom of action arguing that each country possesses its right to sovereignty. Countries within the international community want the entire UN take an active position on answering threats of cyberattacks. Some of them say that a bigger effort is needed to solve this issue. The current ambiguity related to cyberattacks leaves a few questions regarding the definition and meaning of an attack and its consequences. Without any doubt, these ambiguities help cybercriminals and those who use the internet for malicious purposes to continue committing crimes. (Myers, 2020)

Growing necessities and demands for new rules and approaches to cyberspace have been heard for nearly the past decades. This shift led to different resolutions on cyberspace over the past few years. Currently , cyberspace is considered an extension of international law. This means that cyberattacks are viewed legally the same as physical attacks rather than a separate issue without its own legislation.

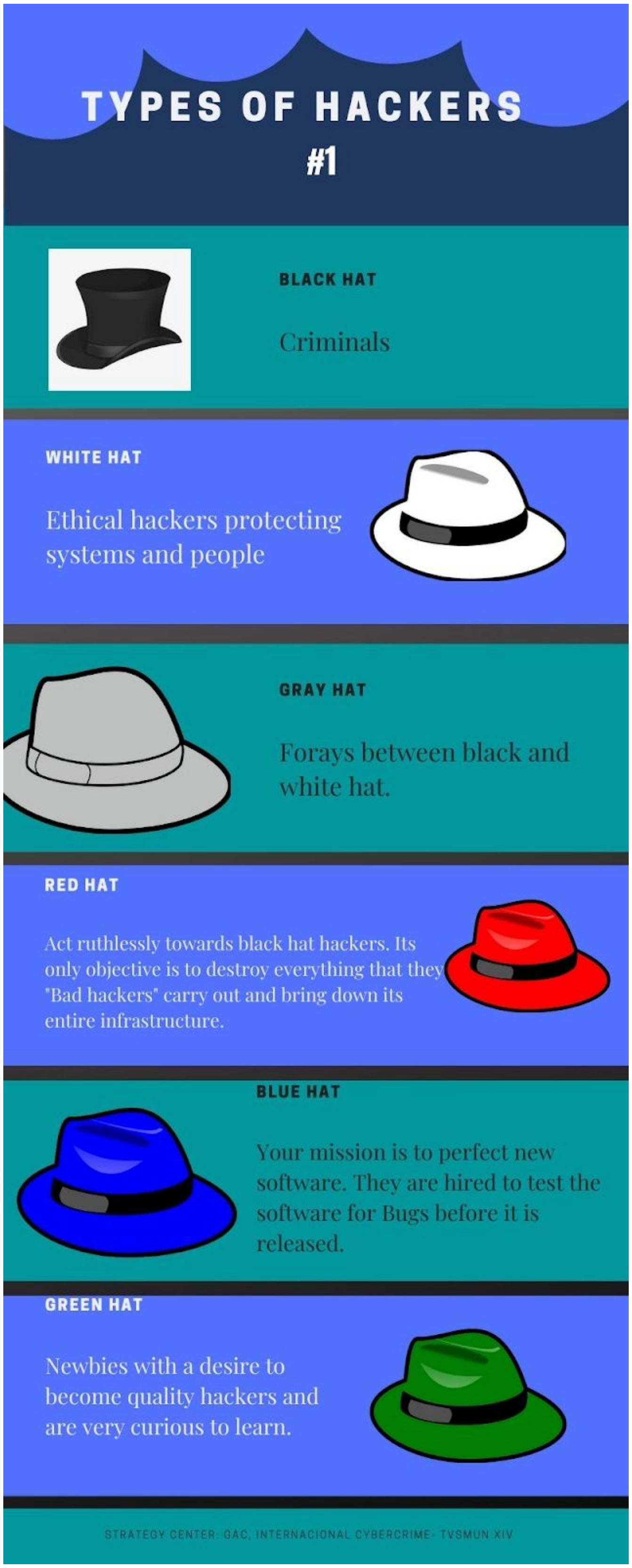
There is some interest in international organisms to address international cybercrime by promoting new international standards. Nevertheless, the disconnection between the global dangers weakens the potential for a forceful international action, even when it is needed the most.

Context

The course of cybercrime in global politics has been on the rise as internet connectivity and different aspects of information technology have spread all over the world. While there is no agreement on an international definition of cyberattack or cyberterrorism within the United Nations, it is important for the cabinet to have a consolidated definition of the term. INTERPOL definies "cybercrime" as a "Sophisticated attacks against computer networks, hardware and software" (INTERPOL, 2021). Following this definition, a cybercrime or a cyberattack must serve a destructive or illicit objective through cyber actions to harm, coerce or intimidate an individual, a population or a state ("Cyberterrorism", 2021). Similar to conventional terrorist attacks, the perpetrators of cybercrime are often difficult to track or identify unless these attacks are claimed by a specific individual or organization. Even today, many attacks remain unclaimed, no matter who is the victim. There have been repeated identifications of the location of the attackers, but the forensic process is often very slow. While an attack can happen in a few instants, the identification of an attacker can take months, under the best circumstances. Over time the occurrences have diversified and intensified, with an increasing variety of more notable attacks being enacted in different countries.

The biggest problem regarding cybersecurity is the speculative nature of the threats. The range of possible threats is quite wide both to governments, intelligence agencies, corporations and individuals. Among of the most known possibilities include:

- Attacks interfering with Internet related networks, installations, etc.
- Attacks on financial industries. Among these are banking and securities trading.
- Interference with critical infrastructure such as emergency services, hospitals, energetic services or transportation.
- Attacks on government systems by criminal, terrorist or organizations looking for information.



TYPES OF HACKERS #1

BLACK HAT

Criminals

WHITE HAT

Ethical hackers protecting systems and people

GRAY HAT

Forays between black and white hat.

RED HAT

Act ruthlessly towards black hat hackers. Its only objective is to destroy everything that they "Bad hackers" carry out and bring down its entire infrastructure.

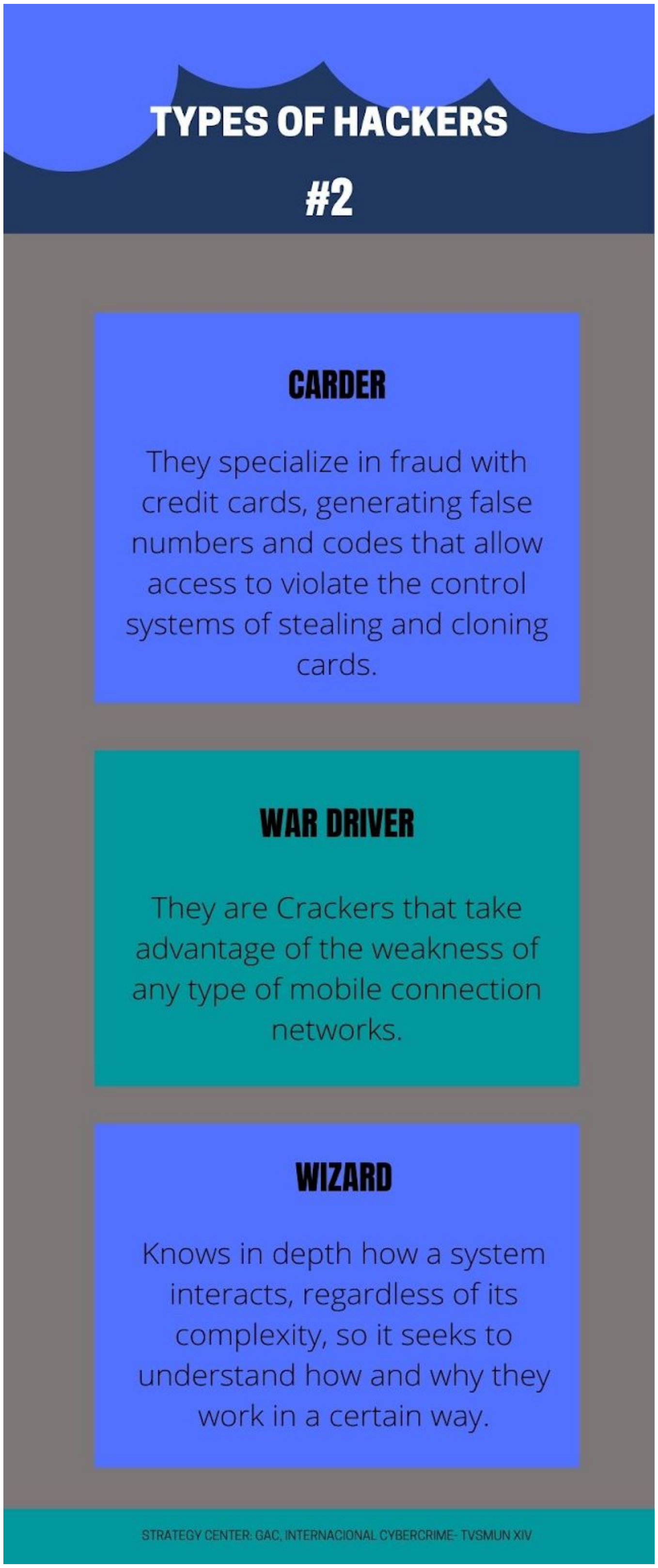
BLUE HAT

Your mission is to perfect new software. They are hired to test the software for Bugs before it is released.

GREEN HAT

Newbies with a desire to become quality hackers and are very curious to learn.

STRATEGY CENTER: GAC, INTERNACIONAL CYBERCRIME- TVSMUN XIV



TYPES OF HACKERS #2

CARDER

They specialize in fraud with credit cards, generating false numbers and codes that allow access to violate the control systems of stealing and cloning cards.

WAR DRIVER

They are Crackers that take advantage of the weakness of any type of mobile connection networks.

WIZARD

Knows in depth how a system interacts, regardless of its complexity, so it seeks to understand how and why they work in a certain way.

STRATEGY CENTER: GAC, INTERNACIONAL CYBERCRIME- TVSMUN XIV

Although there have been various cyberattacks from non-identified criminal organizations, the groups most likely to carry out a cyberattack are powerful countries like China, Russia and the United States. These states are powerhouses in the offensive and defensive use of Information and Communication Technologies, capable of using cybernetic weapons. However, the playing field is opening since different organizations have risen to try to combat cybercriminals . Among these are included international organizations such as the UN Office of Counter Terrorism (UNOCT), the International Telecommunications Union (ITU) and International Police Organizations such as Interpol. In most of the cases, these nongovernmental organizations. are much more successful in dealing with cybercriminals and cyberattacks simply because they are not tied up to an international system and have more capabilities not only to track and diagnose them but also to prevent them.

Cybercrime often has an international dimension. In investigations against cybercrime, it is very important to establish close cooperation mechanisms between countries that are implicated or are the target of a cyber attack. Current mutual legal assistance agreements are based on long-term and rigid formal procedures. Therefore, it is important to articulate procedures and strategies to give a forceful response to cyberattacks as well as requests for international cooperation.

A number of countries base their spectrum of legal aid on the "double criminality" principle. Investigations at the planetary level are generally limited to criminalized crimes in all the countries that are involved. Although there are a certain specific number of crimes that can be prosecuted anywhere in the world, regional differences between each criminal system play an important role. A clear example of this is illegal content. Material that can be legally distributed in one country can easily be illegal in another. Therefore, it is important for delegates to take this into account when taking joint action within the committee to combat cybercrime (Unión Internacional de Telecomunicaciones, 2009).

The current computer technology used today is basically the same all over the planet. Beyond the issues of languages and power adapters, there is very little difference between computer systems and cell phones sold around the world. Due to the normalization of the situation and the use of the Internet, the vast majority of the procedures used in developing countries are the same as those used in developed countries. Standardization allows users around the world to access the same services over the Internet. The fundamental question lies in determining the consequences of the standardization of global technical regulations on the development of the criminal jurisdiction of each of the countries. Similarly, users have the same access to illegal content from anywhere in the world, which allows them to access information legally available abroad that could be illegal in their country of residence (or vice versa).

In theory, developments derived from standardization go beyond the globalization of technology and services and could lead to the harmonization of national laws (International Telecommunications Union, 2009). However, as seen in the negotiations on the First Protocol of the Council of Europe on Cybercrime, national legal principles take longer to change than technical developments (Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, 2003).

While the Internet does not recognize border controls in most cases, there are means to restrict access to different sources of information. The access provider can generally block certain web addresses and the service provider that stores a web address can block users from accessing certain information based on IP addresses linked to a particular country (this is called "determination by). While both measures can be implemented and carried out effectively, they are instruments that can be used to maintain borders in a network that appears to have none.

Current situation:

Study Cases

Most of the recent cyberattacks have been largely attributed to a variety of cybercriminals and a few terrorist organizations, but there have been prominent attacks by states against others over the course of the past four decades. Below are some of the most important examples of attacks designed to disrupt information networks, access critical materials, destroy data, or mislead the citizenship of various countries.

1. *Cyber attacks against the Islamic Republic of Iran in 2009*

   Between 2009 and 2010, The United States and Israel launched a dangerous virus known as Stuxnet against Iranian nuclear enrichment centrifuges and its nuclear fuel facility at the city of Natanz (Sanger, 2012) which is located at the south of Tehran. The Stuxnet attack shut down 10% of Iran's uranium storage facilities for a full year and set back Iran's nuclear project even longer. It is thought that the virus had operated through flash drives. The event got public because a programming error allowed it to escape Iran's Natanz nuclear plant and sent it around the world via the Internet. (Sanger, 2012). Even ten years later, Stuxnet remains as one of the most successful and visible examples of what a cyberattack can cause on a larger scale. Until today, this cyberattacks has been an object of praise and condemnation within the international community.

2. *Russian involvement in the 2016 US presidential election*

   The United States government announced in October of 2016 that it was "confident Russia orchestrated the hacking of de Democratic National Committee and other political organizations such as the Democratic Party”. Those hackings resulted in the public release of thousands of stolen emails. Most of them, including damaging revelations about the Democratic Party and its nominee for the US presidency, Hillary Clinton. Additionally, in December of 2016, Intelligence Agencies such as the CIA, suggested that the objectives of these efforts was to improve Trump's chances for the presidency and hurting Clinton's. This conclusion was based on the latest and complete analysis on the Russian hacking, including the finding that Russian hackers breached GOP individuals and organizations prior to the election. There was also evidence that entities connected to Russian government were financing "troll farms". Their objective was to spread fake news about the Democratic nominee Hillary Clinton. Investigators also found digital footprints of individuals tied to the Russian government who had been seeken be the Intelligence Agencies before. (Diamond, 2016)

3. *Ukraine's 2014 Presidential election*
   Ukraine has often been described as "Russia's Playground". Also, it has become a "test bed" for cybercrime and cyberattacks aimed at damaging infrastructure. (Cerulus, 2019). *"Three days before Ukraine's 2014 Presidential election, Russia hacked into the Central Election Commission and disabled part of its network. Since then, there have been several major cyber-attacks on Ukraine, including on a power grid that affected 230,000 people. Russian entities hacked into Ukrainian tech firms to access banks, airports, and government agencies in Ukraine, costing Ukraine upwards of USD 10 billion." (Myers, 2020)*

These are just samples that demonstrate cyberattacks are a large scale means of projecting state power to negatively impact another state, community, or group of people no matter in which place they are located. The inability of the victim to rapidly identify their attacker makes these crimes much more difficult to solve.

Remarkable UN Resolutions

Over the past several years, the UN has attempted to address cybersecurity through resolutions in its mains organs such as the Security Council and the General Assembly. Even though very few have generated a noticeable impact within the field of cybersecurity to solve the problem on a large scale, they remain influential because they represent the most significant efforts to do something regarding cyber issues.

- **Security Council Resolution 2341:** It was approved by the Security Council in 2017. It established a process, to promote "best practices" to protect critical infraestructure from cyberattacks in coordination with other international organisms such as Interpol and the Un Counter Terrorism Centre . Through this resolution, states stay informed about the potential threats cybernetic attacks represent. Delegates may check the full resolution in the following link: https://digitallibrary.un.org/record/858856?ln=es
- **General Assembly resolution 74/173 (2019):** Focused on development of capacity building of each country to address and respond to cybercrime in components of cooperative objectives (*Resolution adopted by the General Assembly on 18 December 2019*, 2020). Delegates may check the full resolution in the following link: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/429/96/PDF/N1942996.pdf?OpenElement
- **General Assembly resolution 73/266 (2018):** Focused on the development and codification of global standards for cyberspace, with particular focuses on the financial impacts of it and settling responsible State behaviour in the context of international cybersecurity (*Resolution adopted by the General Assembly on 22 December 2018*, 2019). Delegates may check the full resolution in the following link: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement
- **General Assembly resolution 73/187 (2018):** Focused on countering criminal activity. Through this resolution, the General Assembly seeks to stop criminal organizations utilizing communication platforms online to commit crimes both to a national and transnational level. It also calls for improving technical infrastructure especially in

developing countries to address cybercrime and strengthen cybersecurity (*Resolution adopted by the General Assembly on 17 December 2018*, 2019). Delegates may check the full resolution in the following link: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/53/PDF/N1845053.pdf?OpenElement

These measures demonstrate an attempt by the international community to solve this problem. But beyond solving it, what they illustrate is the importance of adopting different policies at the state level and the potential risk for states to ignore them.

SPECIAL PROCEDURE OF GAC

It is composed by:

Directive chair

The directive chair is responsible to be the head of the debate carried on by the delegates and filling in as a first channel for the mandates sent. The presidents should respond to questions that the delegates might as well have regarding the matter, the committee procedure and impact of the mandates on the progression of the debate. Additionally, chairs have the job of supporting their committee in crisis circumstances. For instance the chair might also play the job of crisis delegates or vital jobs in emergencies led by the crisis center.

Strategy center

The principal goal of the crisis staff is to control the actions taken by the committee and its representatives. These activities are brought out through orders sent by the delegates. The mandates initially experience the presidents to be assessed as the main channel, and afterward they are sent to the crisis center, who gives the final word and will choose whether or not they are proper in the debate. Assuming this is the case, your job will be to decide the results of the moves that have been made, including how the overall activities will affect different characters. They are additionally accountable for making and carrying new crises to the committee following the crisis arch.

Bans

Ban 1: *Intelligence Agencies Leaders*

Ban 2: *Cyber criminals*

Delegates

Delegates will speak taking the position of explicit characters yet in addition they could also take the position of nations-states or different associations, which implies that actions taken must be in understanding not just with the interests of the body or advisory group, moreover with individual interests. That is, it must look for answers for the overall goals of the advisory group, while in doing so it likewise tries to accomplish those targets that are on its own plan. Agents must oversee two sorts of plans inside the committee: an open plan and a private plan that seek for their interests regarding the present crisis. Delegates should likewise deal with their plan in a way that shows both their arrangement as agents on the issue and simultaneously a clever utilization of the apparatuses and assets accessible to them inside the committee.

Crisis arch

The alleged Crisis Arch is the committee timeline, which incorporates and contains the most transcendental crises that happen all through the debate, these crises are high-impact events within the theme that the committee must contain. However, the curve isn't static and is liable to changes contingent upon the actions taken by the delegates. These may create a new crisis in the debate or supplant some inside it.

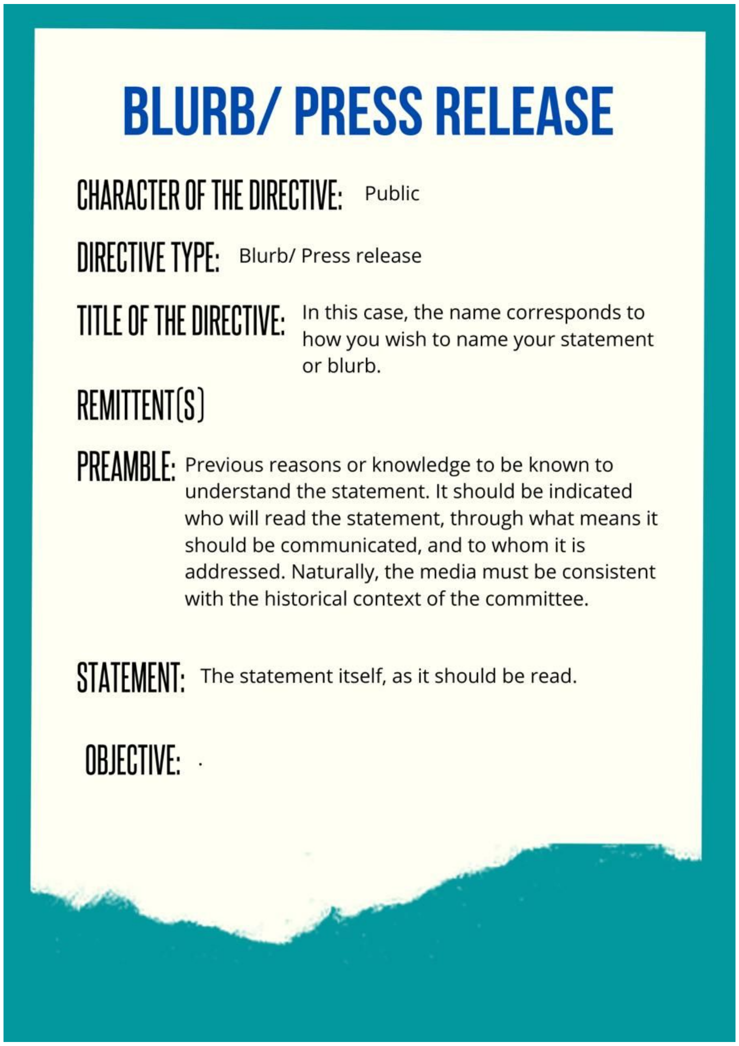
Special Motions:

Consult to the gabinet: By means of this, the committee recognizes a delegate, who can also be the same one who made the motion, to act as moderator of the debate, giving the floor at their discretion without a time limit per speaker. This must be submitted to a voting process in which it will be executed from the decision of a simple majority.

STRATEGY NOTES

Taking into account the global situation with regard to the pandemic, the method that will be used to make ***directives sent will be by a Google Forms****, which will be sent to them so that they can write their actions*

BLURB/ Press release: They are authentic articulations by a delegate, a few characters or the whole Cabinet, they are used to give proclamations, they can range from a specific side or both sides to a group, faction, or the general public in the context of the committee. Its general structure is as follows:



BLURB/ PRESS RELEASE

CHARACTER OF THE DIRECTIVE: Public

DIRECTIVE TYPE: Blurb/ Press release

TITLE OF THE DIRECTIVE: In this case, the name corresponds to how you wish to name your statement or blurb.

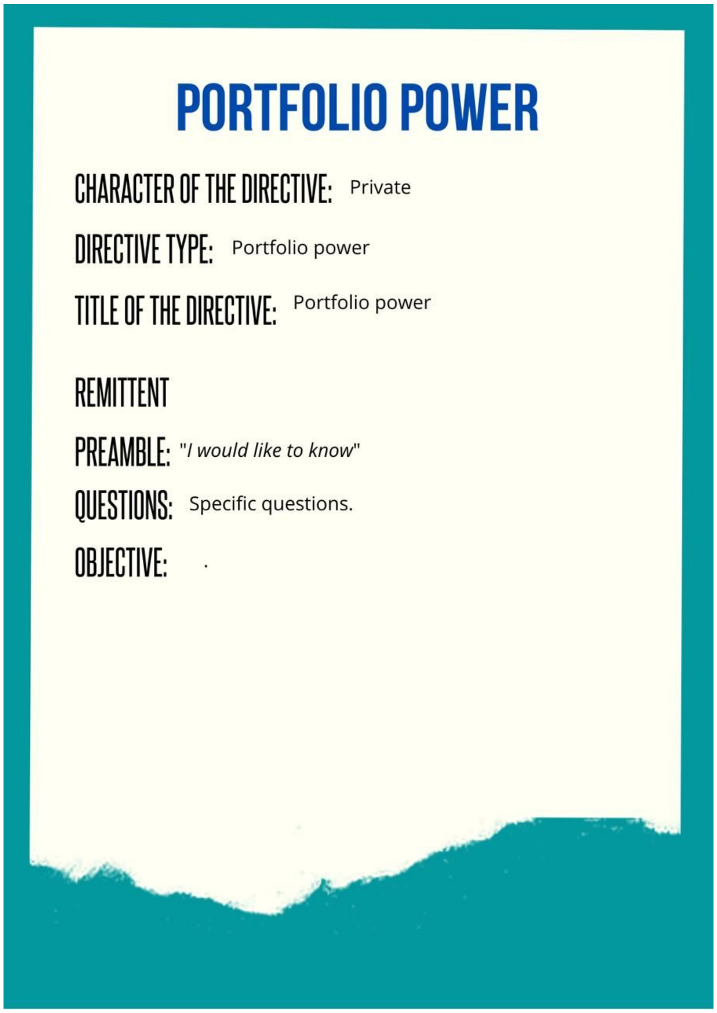
REMITTENT(S)

PREAMBLE: Previous reasons or knowledge to be known to understand the statement. It should be indicated who will read the statement, through what means it should be communicated, and to whom it is addressed. Naturally, the media must be consistent with the historical context of the committee.

STATEMENT: The statement itself, as it should be read.

OBJECTIVE: .

Power of portfolio: At the moment in which any character wants to know something related to the viability of any action or his economic, political, humanitarian aid or any other kind of capacity, he can make use of this mechanism which will be answered by the strategy center with the requested information. They obey the following structure:



PORTFOLIO POWER

CHARACTER OF THE DIRECTIVE: Private

DIRECTIVE TYPE: Portfolio power

TITLE OF THE DIRECTIVE: Portfolio power

REMITTENT

PREAMBLE: "*I would like to know*"

QUESTIONS: Specific questions.

OBJECTIVE: .

Directives:

It is the tool by which delegates can take actions of any sort, as long as they are steady with the limit of the character to be described. They are separated into private and public, these reports must be submitted and recorded as a hard copy and endorsed by the committee. (It is important to note that only public directives are put to a vote.) All mandates that are of a private sort must contain a current encryption technique determined in the header of this, else it will be uncovered by the Strategy Center to the whole committee. All orders ought to be as explicit as could be expected under the circumstances.

The types of directives are:

Spying: The purpose of this is to obtain valuable information from the opposing ban, which can be used to strengthen the strategy of the public agenda of the ban or the private agenda of each of the members. For this to be effective, it is necessary to specify in detail a clear method and plan of espionage, time in which the interception of the databases or platforms will be carried out and the persons involved.

Sabotage:

Its purpose is to develop processes by which a modification, destruction, obstructions, or many interventions is made on a computer, mobile, or tablet, with the purpose of obtaining some benefit for the team or the delegate. This may include:

- Carrying out large transactions.
- Make changes to passwords and the hacker is in control.
- Introductive viruses into terminals, sometimes undetectable for users, but for good scientists.

DDoS attack (Denial of Service Attack):

This type of attack takes advantage of the specific capacity limits that apply to any network resource, such as the infrastructure that enables the website, by sending multiple requests to the attacked web resource, with the intention of overwhelming the website’s ability to manage multiple requests and prevent it from working properly.

Economic disturbance: The purpose of this is to affect the economic situation of the opposite side, therefore it is essential to take into account the economic income that the individual and the side have, both their own and the opposite side. To carry out an action of this nature it is important to specify:

- Which actions will be taken to affect the other ban,
- The resources to be allocated for that action,
- And those who develop the action, or if the whole ban will develop it.

Electrical power grid: Electric energy is susceptible to cyber confrontations, so actions of this nature have the purpose of damaging or delaying the other ban from its own electric energy. Electric energy companies can be hacked by training their servers and controlling their information, in this type of directive it must be specified:

- The company you want to hacker and the area you want to affect,
- The time the action will last,
- The resources to be allocated for that action,
- And the purpose of the action, that is to say, how the other ban is to be affected by this action.

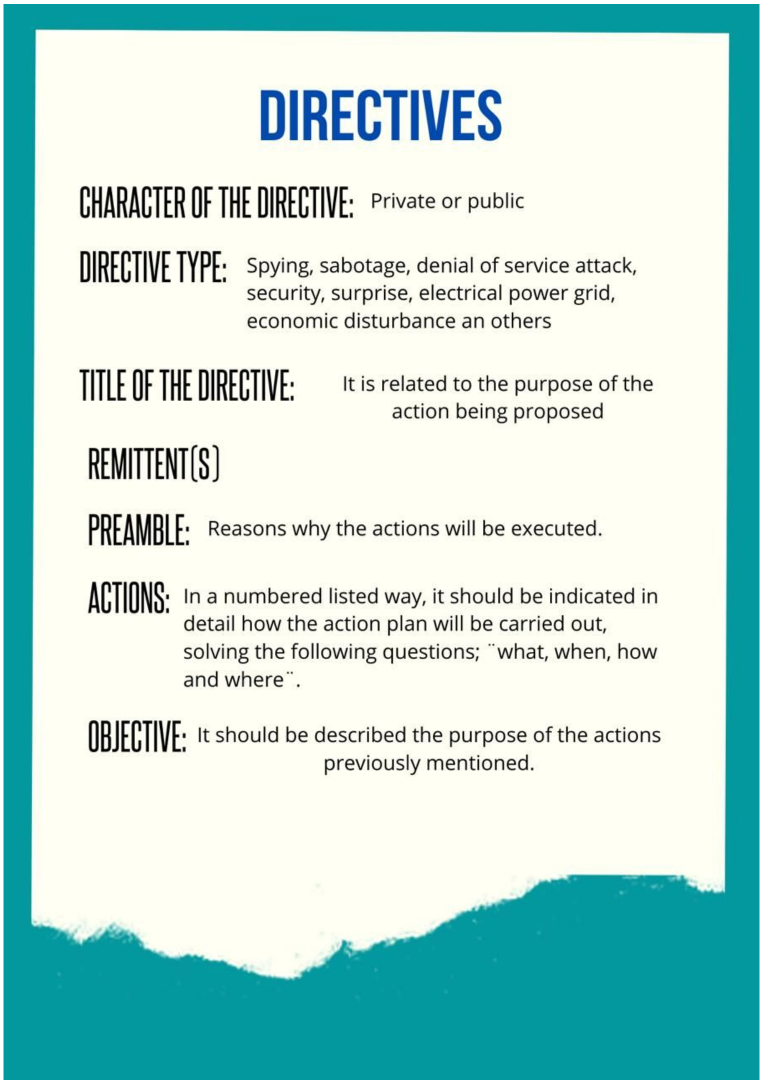
Security: In the case that the ban or the individual is under a situation of risk or attack, and believes that a reinforcement of their security or that of the group to generate is necessary, they will have to specify:

- Character to defend or ban, together with the origin of the defenses,
- The resources to be allocated for that action,
- The defenses to be used and the methods to carry out the defenses,
- And, if any, the strategy to be used or followed.

Surprise: This type of action seeks to be different, that is, it is unconventional and may present a real problem to the opposition, in addition to being innovative, an example of this would be a "cyber day D", "cyber Pearl Harbor" or "cyber 9/11". It must be specified:

- The strategy and the actions to be carried out,
- The resources to be allocated for that action,
- The purpose of the action,
- Place or network where it will be carried out,
- And those who develop the action, or if the whole ban will develop it.

Both, public and private, must follow the structure presented below:



DIRECTIVES

CHARACTER OF THE DIRECTIVE: Private or public

DIRECTIVE TYPE: Spying, sabotage, denial of service attack, security, surprise, electrical power grid, economic disturbance an others

TITLE OF THE DIRECTIVE: It is related to the purpose of the action being proposed

REMITTENT(S)

PREAMBLE: Reasons why the actions will be executed.

ACTIONS: In a numbered listed way, it should be indicated in detail how the action plan will be carried out, solving the following questions; ¨what, when, how and where¨.

OBJECTIVE: It should be described the purpose of the actions previously mentioned.

References

-Council of Europe. (2003). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* [Ebook] (pp. 1-3). Strasbourg. Retrieved from https://rm.coe.int/090000168008160f

- Retrieved 16 January 2021, from https://digitallibrary.un.org/record/858856?ln=es

- Cerulus, L. (2019). How Ukraine became a test bed for cyberweaponry. *POLITICO*. Retrieved from https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

- Cyberterrorism. (2021). Retrieved 14 January 2021, from https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html

- Diamond, J. (2016). Russian hacking and the 2016 election: What you need to know. *CNN*. Retrieved from https://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/index.html

- INTERPOL. (2021). What is the difference? Cybercrime- Cyber-enabled crime. Retrieved 14 January 2021, from https://www.interpol.int/es/Pagina-de-busqueda?search=cybercrime

- Myers, N. (2020). *Cyber Security: Cyber crime, Attacks and Terrorism* [Ebook] (pp. 1-3). Old Dominion University. Retrieved from https://www.odu.edu/content/dam/odu/offices/mun/docs/1st-cyber-attacks-un-day.pdf

- General Assembly. (2019). *Resolution adopted by the General Assembly on 17 December 2018* [Ebook]. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/53/PDF/N1845053.pdf?OpenElement

- General Assembly. (2020). *Resolution adopted by the General Assembly on 18 December 2019* [Ebook]. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/429/92/PDF/N1942992.pdf?OpenElement

- General Assembly. (2019). *Resolution adopted by the General Assembly on 22 December 2018* [Ebook]. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement

- Sanger, D. (2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. Retrieved from https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

- Unión Internacional de Telecomunicaciones. (2009). *El Ciberdelito: Guía para los países en desarrollo* (pp. 13-15). División de Aplicaciones TIC y Ciberseguridad. Retrieved from https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf