SECURITY COUNCIL

SECURITY COUNCIL

Topic A.-

"Cyber security: protection against cyber threats and espionage"

"Global interconnectivity means that the frequency and impact of cyberattacks could be increasingly widespread, affecting an exponential number of systems or networks at the same time" ***- António Guterres***

Cyber threats to the international security environment are becoming increasingly more frequent and sophisticated, and the Security Council acknowledges the importance that must be given to this topic.

Since the year 2019 cyber security has concerned the International Community as the cyber-attacks and threats have increased and led to multiples conflicts regarding the stealing of confidential and sensible information of governments and civilians, and even the use of Information and Communication Technology (ICTs) for terrorist purposes.

Cyber-attack must be understood as an assault, via cyberspace, targeting an enterprise, government or individual's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

This problem has led this committee's members to hold internal meetings with the purpose of strengthening their systems and informing about the effects that ICTs have, and what action plans may be carried out in order to prevent and fight against the cyber threats countries have been receiving, carrying out its first official meeting on this matter in June 2021.

2022 has been a year in which cyber attacks have increased significantly, since a massive exploitation of one of the most serious vulnerabilities on the internet, “theApache log4j”, and a full-blown cyber warfare from the Russia-Ukraine war. This led to the incasement in the second quarter of 2022 by 32%, compared to the second quarter of 2021, giving a weekly average of 1.2K cyber attacks worldwide.

The United States, The United Kingdom and India are the countries who have suffered most cyber attacks in the last decade, followed by Germany, South Korea and Australia. These attacks have had many known purposes, although, the main have been exploiting a bug in a commonly used email server to infiltrate sensitive data from organizations and governments, as well as the recording of audio and stealing of personal credentials of civilians.

It is important to mention that, the implementation and regulation of cyber security in an International level is complex; innovative approaches must be given, as the Internet control may be limited and even compromised in many countries, which is the reason why this Committee aims to establish a set of guidelines, norms and commitments, in which the entire of the International Community can agree on and implement, with the purpose of guaranteeing safety in the cyberspace.

Given the elevated risks the International Community has suffered and observed in matters of cyber security among nations, this Council calls for a discussion on how international law applies to the use of information and communications technologies by States and which will be the scope of it, reminding that addressing cyber threats requires multilateral cooperation.

GUIDE QUESTIONS:

- **Which international instruments can be applied to cyberspace?**
- **Why would the right to self-defense be at risk if these instruments were applied?**
- **Can International humanitarian law in cyberspace be regulated?**
- **With which other committees could this Council address this matter and ask for support?**
- **Are there any cases in which cyber-espionage should be justified? If yes, which would apply and how?**
- **What sectors of the administration of a country could be found weakened by a foreign cyber-attack?**
- **Can a country be responsible of cyber attacks?**
- **How could a pacific resolution to the intended cyber-attacks be reached?**

SOURCES OF REFERENCE:

- *In Hindsight: The Security Council and Cyber Threats, an Update, February 2022 Monthly Forecast : Security Council Report*. (2022). Securitycouncilreport.org. https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php
- https://www.un.org/counterterrorism/cybersecurity
- https://ccdcoe.org/organisations/un/

- https://www.tandfonline.com/doi/full/10.1080/23738871.2022.2041061
- https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents