Addressing Cyber Crime as a threat to the international system

Topic A

Security Council

AQMUN

FOR AN INCLUSIVE, PROSPERUS AND FAIRER WORLD

2023

Introduction to the committee

According to the San Francisco Charter of 1945 (also known as the Charter of the United Nations), the Security Council (SC) has the primary responsibility for maintaining international peace and security. This Main Body of the United Nations (UN) is made up of 15 full voting members, 5 of them permanent members (China, United States, the Russian Federation, France and United Kingdom), and 10 non-permanent members, elected by proportional geographical representation, in the plenary session of the United Nations General Assembly (UNGA) for a period of two years.

In conformity with the UN Charter, all member states agree to accept and comply with the decisions of the Security Council, which makes this UN body the only one whose decisions are obliged to comply with. Situation that makes it the request of collective security, and scenario of international politics on a global scale (art. 25, UN, 1945).

Based on this logic, it is up to the SC to ensure the most important of the principles of this organization, contained in the first article of its charter: Maintain international peace and security and with it: “take effective collective measures to prevent and eliminate threats to peace, to suppress acts of aggression or other breaches of peace; and achieve by peaceful means. In accordance with the principles of justice and international law, the adjustment or settlement of disputes or international situations is likely to lead to breaches of peace” (UN, 1945).

Globalization and technology

Over the last few years, new technologies have been developed, giving place to a significant digital transformation and changing the way we interact in this globalized world. The main characteristic of technology is facilitating processes of the human being's daily work and reducing costs. However, if it is not well managed, it can be very risky thanks to the interdependence of the actors. Impacting in diverse areas that are evolving constantly. This makes international actors face new challenges and opportunities, trying to maximize the benefits from technology and proving their resilience to changes.

Globalization has made access to technology easier, making its use common. Therefore, digitalization of data has become ordinary among nations and as a consequence it has also brought something known as cybercrimes. By the 21st Century, there's hardly anywhere that has not been touched by cybercrime.

Technological globalization is the process by which the same technological tools are developed and used jointly in all countries of the world (Duran et al, 2019).

In the 1970s, the process of what was taking shape in the 1990s began: a cyberworld globalization, which has another space as its platform: Cyberspace, and the different technological and informational innovations. From the global connections of the real world, we have gone to the hyper connections of the virtual cyberworld, moving around in virtual social networks, which forge the actions of the cybernetic subject in cyberspace navigations without the limits and confines of geographic spaces, but with a cyber geographic vision.

The United Nations Development Programme (UNDP), in its Human Development Report (1999), tells us that politics, technology, culture and the economy of countries are part of a globalization, totally different to that of the beginning of the 16th century and the end of the 20th century, which has come to configure a global cyberworld. The Report sets out three distinct ways in which the landscape of globalization has changed:

• Space reduction. People's lives—their jobs, their income, and their health—are affected by events on the other side of the world, often by events they don't even know about.

• Time reduction. Markets and technologies are now changing with unprecedented speed, with action taking place at a distance in real time and effects on people living far away. For instance: the rapid reversal of capital flows from East Asian markets and their contagion from Thailand to Indonesia and Korea, as well as for South Africa.

• Disappearance of borders. National borders are being eliminated, not only with respect to trade, capital and information, but also with respect to ideas, norms, culture and values.

This cybernetic globalization is part of our life, whether to affirm it as a hyperconnection of an increasingly complex world in economic, cultural, technological and social terms, or to reject it within its own virtual networks, as part of a local dynamic, of a specific country, which was once the benchmark against others.

That is why globalization, is interconnected to the economy, politics, technology and culture, and would not have been possible in the world without the entry of the cyberworld, giving rise to cyberspace and its different levels of depth in terms of information, images, writing, social networks and virtual communities (Marejo, 2017).

Cybercrimes

Cybercrime is the use of computers and the internet as instruments to commit illegal actions, violating the confidentiality and integrity of data. For instance, fraud, trafficking intellectual property

and stealing identities. The attacks are made in a virtual body which defines the virtual identities made up of numbers, identifiers and databases, being essential in this virtual age.

These crimes have grown in importance as governments, commerce and entertainment have made the computer central. Cybercrime has made evident how fragile the centrality of networked computers is in apparently solid data. Cybercriminals have taken advantage of it by being agile and organized, trying new technologies and cooperating to make possible the attacks now that there's a great impact on the online systems, networks and infrastructure of governments, business and individuals.

Cybercrime is one of the fastest growing transnational crimes facing INTERPOL member countries. While the rapid evolution of the Internet and information technology have enabled economic and social growth, increased reliance on the Internet has created more risks and vulnerabilities, and has opened up new possibilities for criminal activity.

Therefore, adversaries developed cyber capabilities to exploit human or security vulnerabilities and seek for gaps in intelligence and information security networks. The existence of diverse ways and more sophisticated techniques of cybercrimes are increasing, meaning a rising threat for national and international security. Crimes are interconnected by organized groups, which makes cybercrime just another option and fuels the proliferation of committing illegal actions which affect non-digital areas such as business and hence in economies all around the world.

The “borderless” nature of cybercrime means that law enforcement agencies have trouble responding effectively, due to limits on cross-border investigations, legal issues, and the diversity of capabilities around the world.

Unlike other investigations, in many cybercrime cases the digital evidence is found primarily in the private sector, which operates and maintains many parts of the Internet's infrastructure. Therefore, it is essential to collaborate between different stakeholders in order to address new cyber threats (Interpol, 2023).

It is extremely important to note that Cyberdefense not only has a preventive role against attacks as Cybersecurity does, but also seeks to respond to them with new attacks in order to safeguard security.

Cybersecurity in the international system

The international system is dependent on the decision making of different actors such as organizations and nations. The national variables affect the international sphere, which indicates the

need to create an international security based in cooperation that also addresses the problems related to cybercrimes.

One of the biggest challenges about cybercrimes is the absence of geographical limits, cybercrimes know no national borders. Victims, criminals and technical infrastructure reach multiple jurisdictions, making the investigations and prosecutions of the responsibles complex. This sets severe problems for law enforcement since these crimes now require common legal frameworks established among nations.

Cyber threat intelligence has become essential and is now a main mechanism where nations collect information based on past experiences and research made about cybercrimes, to then use it to secure the databases.

Global response

Battling criminals who hide in relative anonymity and are constantly trying to disrupt the actual order in cyberspace, is a priority to maintain peace in the international system. As a resolution for this major problem, The United Nations Office on Drugs and Crime (UNODC) is the main organization, with a set of mechanisms to fight against cybercrime. As well as multiple instruments that establish international law enforcement cooperation (bilateral, multilateral, regional, continental or universal). For instance:

- Council of Europe's Convention on Cybercrime of 2001.
- The Commonwealth of Independent States' Agreement on Cooperation in Combating Offences related to Computer Information of 2001.
- The Arab League's (League of Arab States) Arab Convention on Combating Information Technology Offences of 2010.
- The Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security of 2010.
- African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa of 2012.
- African Union Convention on Cyber Security and Personal Data Protection of 2014.

All of this is part of a broader cybersecurity approach, risking the infrastructure of the world as we know it. These instruments have the objective to close gaps where criminals can take advantage of, by sharing intelligence and coordinated action. There are also specific security organizations that collaborate to enable intelligence and law enforcement responsibilities worldwide. Developing techniques and analytic tools in order to reduce cyber threats. Some of the leading organizations are FBI, INTERPOL, US Secret Service and Europol, which are in charge of preventing, detecting,

investigating and disrupting cyber crimes by building cross-sector partnerships to create a safer world.

Guiding questions

- What actions can your country take based on international treaties?
- Is cybersecurity a priority for your nation?
- Has cybercrime violated the security of your country?
- What type of mechanisms are used to protect the information of users?
- Which are the most frequent cybercrimes that affect security?
- Are your instruments of protection effective?
- Do you consider essential alliances for preventing cyberattacks?

References

Cybercrime as a threat to international security. (2018, July 16). ISPI. Retrieved December 14, 2022, from https://www.ispionline.it/it/pubblicazione/cybercrime-threat-international-security-20995

Cybercrime as a threat to international security. (n.d.). United Nations Office on Drugs and Crime. Retrieved December 14, 2022, from

https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html

Cybercrime | Definition, Statistics, & Examples. (n.d.). Encyclopedia Britannica. Retrieved December 14, 2022, from https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy

Cyber Crime. (n.d.). Federal Bureau of Investigation. Retrieved December 15, 2022, from https://www.fbi.gov/investigate/cyber

Cyber crime. (n.d.). National Crime Agency. Retrieved December 15, 2022, from https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Cybercrime trends in 2022 | DW Observatory. (n.d.). Digital Watch Observatory. Retrieved December 14, 2022, from https://dig.watch/topics/cybercrime

DURAN, D. ahin et all, 2019. Global Challenges in Public Finance and International Relations [en línea]. 1a Edicón. Tokat, Turquía: IGI Global. Advances in Finance, Accounting, and Economics. ISBN 9781522575641. Disponible en: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-7564-1

Interpol. (n.d.). *Cybercrime*. Retrieved December 14, 2022, from https://www.interpol.int/Crimes/Cybercrime

INTERPOL, 2022. Ciberdelincuencia. Delitos [en línea]. [Consulta: 1 febrero 2023]. Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia.

MEREJO, A., 2017. La globalización del cibermundo. trilogía Ciencia Tecnología Sociedad [en línea], vol. 9, no. 17, pp. 175-187. ISSN 2145-7778. DOI 10.22430/21457778.634. Disponible en: https://revistas.itm.edu.co/index.php/trilogia/article/view/634.

¿Qué es ciberseguridad y ciberdefensa? (n.d.). NLT Secure. Retrieved February 24, 2023, from https://www.nltsecure.com/blog/que-es-ciberseguridad-y-ciberdefensa

United Nations. (n.d.-b). *United Nations Security Council |*. Retrieved February 1, 2023, from https://www.un.org/securitycouncil/

UNODC, U.N.O. on D. and C., 2023. Cybercrime. Office on Drugs and Crime [en línea]. [Consulta: 1 febrero 2023]. Disponible en: https://www.unodc.org/.