CYBERSECURITY, CIBERCRIMINALITY

AND TRANSNATIONAL ORGANIZED CRIMINALITY

1) THE CONCEPT OF CIBERSECURITY

Cybersecurity refers to a protocol of measures designed to protect the cyberspace environment (systems, programs, networks and hardware) from being accessed by cybercriminals looking for assets and information stored on devices such as computers and smartphones, as well as other online storage means in clouds, in order to obtain illicit gains and to increase the range of their criminal activities: Forgery and data tampering; online misappropriation and theft (bank fraud); Computer hacking and data theft; Storing, possession, production, distribution and reproduction of videos and pictures containing child pornography; Sexual harassment and solicitation involving children; Cyberterrorism; Threat; Distribution of adult and/rape-related/pornography; Service interruption; Cyberbullying (creating and publishing fake profiles, dissemination of offensive texts on blogs and virtual communities); Incitement and praise to crime; Hate crimes; Crimes against intellectual and artistic property; Illegal commercialization of medications.

Indeed, public security agencies must be prepared to face this type of organized and transnational crimes, hence the need for our alliance, as promoters of justice, for the sake of public safety, combining efforts of the entire justice system in defense of the democratic state of law, human rights, and international cooperation, to ensure a quick and protective response to cybercriminal offenses.

Living in the Information Age and dealing with cybercrimes has deemed necessary the concern with pre-existing illicit behavior as well as new ones practiced online, which have altered geographic limits and redesigned borders.

In 2020, the National Cyber Security Strategy, or E-Cyber was approved in Brazil, by means of Decree 10,222 of February 5, 2020. It actually works as a guideline for public policies within the Executive Branch, an improvement of the original Cybersecurity legal framework.

2) CYBERCRIMINALS

According to UNODC – United Nations Office on Drugs and Crime, cybercriminals have been able to capitalize on the anxieties and fears of their victims, taking advantage of the large number of online workers who often have outdated security systems. This new reality has also led to an increase in the rates of online exploitation of women and children.

These criminal individuals act alone as well as withing criminal organizations, some of them international.

Even terrorist groups use new methods and technologies to diversify their means of financing, communicating, and operating, which include the use of cyber currencies, drones and safeguarded messaging platforms on the Deepweb/Darkweb.

3) ORGANIZED CRIME

National and transnational organized crime structures operate through a network in order to increase their efficiency in committing crimes, enlisting public agents, and protecting its members from the forces of law and order. This network acts in a coordinated way in laundering of money and uses the Internet to simplify financial transactions with capitals obtained from crimes, allotting benefits to all of those involved, including the corrupt public officials, who are necessary to hinder the work of honest authorities.

4) TRANSNATIONAL OFFENSE AND ITS IMPLICATIONS ON THE STRUCTURE OF THE ECONOMY AND ON LEGAL SECURITY

These crimes committed by criminal groups and their agents in several countries have cost billions in damages to lawful financial systems nationwide, either directly, when financial agents are victims of thefts, such as bank fraud and hacker attacks on banks; and indirectly, when they transact goods or services obtained through cybercrimes.

This is reported by the president of ARME, Cape Verde's Multisectoral Regulatory Agency for the Economy, when he says that there is an exponential increase in cybercrimes worldwide, and that Cape Verde is no exception. He claims that, in 2015, the world lost about three trillion dollars to cybersecurity and cybercrime issues and adds that, in 2021, the estimated losses were about six trillion dollars.

5) WAYS OF FIGHTHING IT

- Training of law enforcement agents, in investigative techniques to operate in open networks and in the Deepweb/Darkweb.
- Creation of specialized groups, in the units of the Federal and State Prosecution Offices, and of technical core groups, with training and qualification of their members.
- Greater commitment from online services providers – development of filters and security tools.
- Participation of Brazil in the Budapest Convention – Intensification of cooperation deals between countries to expedite the obtention of evidence.

6) CRIME PREVENTION AND CRIMINAL JUSTICE

In accordance with UNODC: development and implementation of more effective legal agendas, policies and programs to combat transnational organized crime; in line with the United Nations Convention against Transnational Organized Crime and its Protocols.

Actions in crime PREVENTION, both in the social area (workshops/seminars for school and university teachers; campaigns, etc.) and legislative (study groups and in Parliamentary Inquiry Commissions).

7) THE SUBJECT OF PARTNERSHIPS

Maintain the articulated efforts between public agents, prosecutors of justice, law enforcement, the justice system, and the private sector along with the civilian, academic and scientific communities, and other relevant parties, which proved to be essential for battling criminal organizations.

Promote, at national, regional, and international levels - with due respect for national legal structures and the principles of international law - collaborations between both the public and private sectors with the digital industry, the financial sector and communication services providers, in order to enhance international cooperation in the fight against cybercrime.

8) THE UNITED NATIONS ADDRESSING THE ISSUE

The Kyoto Declaration on Advanced Crime Prevention, Criminal Justice, and the Rule of Law: Towards Achieving the 2030 Agenda for Sustainable Development presents the importance of the topic for the UN. This document asserts:

> 1 We express deep concern about the negative impact of crime on the rule of law, human rights, socioeconomic development, public health and security, the environment and cultural heritage;

2 We also express deep concern that crime is becoming increasingly transnational, organized and complex and that criminals are increasingly exploiting new and emerging technologies, including the Internet, to carry out their illicit activities, thus creating unprecedented challenges in preventing and combating existing crimes, as well as new and emerging forms of crime;

3 We undertake to contribute to achieving the 2030 Agenda for Sustainable Development through our efforts in crime prevention and criminal justice, with the firm recognition that sustainable development and the rule of law are interlinked and mutually reinforcing, that crime is an impediment to sustainable development and that achieving sustainable development is an enabling factor for States to effectively prevent and combat crime;

(...)

5. We undertake to intensify concerted global efforts to prevent and combat crime, facilitating and strengthening international cooperation in criminal matters;

9) THE FIGHT OF BRAZIL'S FEDERAL PROSECUTION OFFICE

Actions taken by the MPF (Federal Prosecution Office) in Brazil on the subject. A special mention to the industrious performance of the Support Group concerning Cyber Crimes of the 2nd Coordination and Evaluation Criminal Court of the MPF.

This Court has published two relevant works on the subject:

1 - CRIMES CIBERNÉTICOS. COLETÂNEA DE ARTIGOS. Volume 3, 2018.

2 - ROTEIRO DE ATUAÇÃO. CRIMES CIBERNÉTICOS E PROVAS ELETRÔNICAS, 4th edition, updated and expanded, 2021.

10) TYPES OF CYBERCRIMES

Even before Brazil acceded to the Budapest Convention, the Brazilian Legislation presented the following types of digital felony: Forgery and data tampering; Online misappropriation and theft (bank fraud); Computer hacking and data theft; Storing, possession, production, distribution and reproduction of videos and pictures containing child pornography; Sexual harassment and solicitation involving children; Cyberterrorism; Threat; Distribution of adult/rape-related pornography; Service interruption; Cyberbullying (creating and publishing fake profiles, disseminating offensive texts on blogs and virtual communities); Incitement and praise to crime; Hate crimes; Crimes against intellectual and artistic property; Illegal commercialization of medications.

To these must be added the criminal categorizations of the Budapest Convention.

11) THE IMPORTANCE OF INTERNATIONAL COOPERATION

International cooperation is essential in the fight against crime, and Brazil's adherence to the Budapest Convention includes the country into the international legislation, for the speedy resolution of crimes relating to the Internet.

12) AT THE BUDAPEST CONVENTION AND THE COUNCIL OF EUROPE, INTERPOL AND THE OECD

BRAZIL'S COMPLIANCE TO THE CONVENTION ON CYBERCRIME, HELD IN BUDAPEST, ON NOVEMBER 23, 2001, WAS APPROVED BY LEGISLATIVE DECREE No. 37, OF DECEMBER 17, 2021.

> **The Cybercrime Convention, which encompasses more than 65 assenting countries, is currently the main tool for aligning the categorization of cybercrimes, for the provision of the necessary apparatuses for the effective prosecution of cybercrimes, as well as cooperation between nations, for the fast obtention of electronic criminal evidence.**

The Convention, therefore, by means of its Cybercrime Committee (T-CY) and various subcommittees, enables the constant discussion and evolution of its provisions, keeping its interpretation up to date. Through the training office, the C-PROC, it offers several training courses, meant for participating and prospective-member countries, all designed to promote the alignment of the various practices regarding criminal prosecution of cybercrimes and obtainment of electronic evidence, especially between countries, in order to improve the effectiveness of the state's response to cybercrimes.

The Convention is comprised of 48 articles, divided into four chapters, which deal with terminology, criminal provisions, criminal procedure, and international cooperation. Great emphasis is placed on aligning criminal legislation, a cornerstone for expanding cooperation between countries, establishing tools for authorities to investigate and prosecute cybercrimes and other crimes involving electronic evidence more effectively; as well as on cooperation between countries, whether for the exchange of evidence, or for the extradition of persons, in recognition of the international nature of cybercrimes and the peculiarities of electronic evidence.

CONCLUSION

Moved by a spirit of unity and concerned with the common good, we have worked on designing the program with the theme of the Seminar on CYBERSECURITY, CYBERCRIMINALITY AND TRANSNATIONAL ORGANIZED CRIME, as believers of disseminating knowledge and discussing this essential topic, for the benefit of humanity, due to the effects that the vulnerability of cyberspace have on people in today's world.

The Brazilian Prosecution Office - in line with international organizations linked to the UN, and collaborating with prestigious Portuguese Universities, presents ideas, which are proposed for debate, to promote the enhancement of legislative, prosecutorial, and investigative tools, to fight criminals who use the Internet for the commission of all kinds of crimes against humanity, ruining and jeopardizing democracies and, consequently, world safety and peace.

Alcides Martins – Deputy Attorney General of the Republic of Brazil and Managing Director of Escola Superior do Ministério Público da União (Union's Prosecution Office Academy).