THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES: TOWARDS A NEW UNITED NATIONS CONVENTION

Vittoria Pellerito

INDEX

INTRODUCTION ***2***

CRIME IN CYBERSPACE: A NEW ERA ***4***

1.1 CRIME IN THE DIGITAL ERA 4

1.2 CYBERCRIME: DEFINITIONS AND MANIFESTATIONS 9

1.3 THE PROPULSIVE ROLE OF THE UNITED NATIONS IN THE INTERNATIONAL FRAMEWORK AND IN THE FIGHT AGAINST CRIME 18

1.4 HISTORICAL OVERVIEW OF EXISTING INSTRUMENTS 25

1.5 THE NECESSITY OF A UNITED NATIONS INTERNATIONAL CONVENTION ON CYBERCRIME 42

THE ELABORATION OF A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES ***47***

2.1 THE *AD HOC* COMMITTEE 47

2.2 THE FIRST SESSION OF THE *AD HOC* COMMITTEE 51

2.3 THE FIRST INTERSESSIONAL CONSULTATION OF THE *AD HOC* COMMITTEE DEDICATED TO MULTI-STAKEHOLDERS 59

2.4 THE SECOND SESSION OF THE *AD HOC* COMMITTEE 62

2.5 THE SECOND INTERSESSIONAL CONSULTATION OF THE *AD HOC* COMMITTEE DEDICATED TO MULTI-STAKEHOLDERS 68

2.6 CONTEXTUAL DEVELOPMENTS TO THE NEW CONVENTION ON CYBERCRIME 74

THE COMMITMENT OF MULTI-STAKEHOLDERS IN THE AD HOC COMMITTEE ***78***

3.1 THE IMPORTANCE OF THE PARTICIPATION OF MULTI-STAKEHOLDERS AND CIVIL SOCIETY IN DECISION-MAKING PROCESSES 78

3.2 THEORIES AND SUBMISSIONS FROM MULTI-STAKEHOLDERS RELATED TO THE SESSIONS OF THE *AD HOC* COMMITTEE 82

3.3 STATE OF PLAY AND FUTURE PERSPECTIVES OF THE *AD HOC* COMMITTEE 90

CONCLUSION ***92***

ADDENDUM ***94***

BIBLIOGRAPHY

INTRODUCTION

Globalization has determined an impressive diffusion of modern information and communications technologies, allowing the creation of a borderless cyberspace, which overcomes space-time barriers, and where threats are dangerous for all, indistinctly.

Nowadays, cybercrime has become one of the most widespread criminal offences in the world, mainly due to its cross-border nature, entailing that everyone could be subjected to it, from the average citizen to strong institutions.

This type of criminality is none other than the evolution of offences in current times, slipping away from traditional models provided for by national legal systems. For this reason, it is necessary to counter such a transnational crime with equally transnational actions.

This study is based on a detailed analysis on this criminal phenomenon, with particular attention to its various manifestations and the modalities with which each country has faced it.

This thesis represents the belief that a new, global convention countering cybercrime and, in general, the use of ICTs for criminal purposes, is necessary to contrast such a broad and constantly increasing phenomenon. The ineffectiveness of the current countermeasures led world's States to agree on the elaboration of a new international document by the United Nations.

The thesis is articulated in three chapters, the first of which is divided in five paragraphs, on various matters: the phenomenon of cybercrime is analyzed in detail, starting from its origins to its manifestations in cyber-dependent crimes and cyber-enabled crimes. Moreover, references are included on regional and international legislations formulated over time to counter this offence, especially by the United Nations, which had a critical role in recognizing the necessity of a new global convention to counter the use of information and communications technologies for criminal purposes.

The second chapter, composed of six paragraphs, is the result of the writer's participation to the sessions and intersessional consultations dedicated to multi-

stakeholders of the *Ad Hoc* Committee created by the UN General Assembly to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

Finally, the third chapter analyzes the importance of the participation of multi-stakeholders in decision-making processes of the United Nations, fully recognizing the role played by the civil society during the last sessions of the *Ad Hoc* Committee, with also a reference to the future perspectives of the work of the aforementioned Committee.

CHAPTER 1

CRIME IN CYBERSPACE: A NEW ERA

SUMMARY: 1.1 Crime in the Digital Era – 1.2 Cybercrime: Definitions and Manifestations – 1.3 The Propulsive Role of the United Nations in the International Framework and in the Fight against Crime – 1.4 Historical Overview of Existing Instruments – 1.5 The Necessity of a United Nations International Convention on Cybercrime

1.1 CRIME IN THE DIGITAL ERA

The advent of information technologies has involved a radical change within the modern society. Technological instruments penetrated in sectors and systems that regulate social dynamics, such as study through distance learning, or smart-working, or also for common activities like watching a film or reading a book. This is the Digital Era, in which globalization has permitted the development and diffusion of Information and Communication Technologies, indicated with the acronym ICTs.

Since Internet appearance in the nineties, the growth of the use of devices allowed an available divulgation of information, modifying not only relations within communities, but also international ones: in the last few years, a very discussed theme by States is IT security.

Remarkable benefits deriving from the great fruition of technology allow a real knocking down of its borders, overcoming space-time barriers.

Thanks to these new computer instruments, an improvement in the judicial sector was also possible. The efficacy of these means allowed a higher efficiency not only during the investigation phase, for instance through video cameras, or telephone tapping with the use of the concealed microphones, but also during the procedural phase, with the hearings possible remotely, up to the executive phase, with a very incisive control on subjects' behaviors, whose personal freedom is restricted, for example in case of house arrest.

But the other side of the coin, there is the abuse and misuse of Internet and ICTs by the society, leading to both physical and mental issues, and mostly new manifestations of criminality. Besides, crime has accompanied humanity since always: digital revolution has led to a criminal revolution, founding fertile land for new methodologies of assaults to juridical goods, in which technology became a key component[1].

Despite all different definitions formulated, generally Information and Communications Technologies are those electronic instruments, applications and systems that consent to people and organizations to interact actively in the digital world. They are innovative products which function is to elaborate and communicate information through digital means and related technologies, like hardware (physical parts) and software (programs). They contain images, audio files, documents that will be transmitted to receivers, common people.

Actually, current ICTs are a lot, but certainly they may be distinguished in: telecommunication networks, those means through which information are shared. This category alone endured many evolutions, starting from landline phones to Wi-Fi; devices, physical-electronic instruments like computer, smartphone, tablet etc; and, finally web services: indeed, ICTs are not only material tools, but also intangible ones, like search engines, electronic mail and obviously social media[2]. Typical characteristic of these means is immediacy: it is possible put into contact people who are in geographically distant places, as it is possible hear world news in real time, when they happen.

It can be said without a doubt that ICTs have promoted globalization and digitalization phenomena, worldwide. And yet, problems related to these instruments arise in the context of criminality: indeed, ICTs are used as components for the commission of crimes, complementarily, or also directly for the implementation of the criminal conduct.

In some cases, information and communication technologies are used by authors in an accessory way, to facilitate or to agree on modalities of consummation of a crime, such as in the case of involvement of persons in a crime, or associative

[1] R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, Diritto Penale Contemporaneo, 2012

[2] E. TRUZZI, *ICT*, www.nextre.it, 2021

offences, or perhaps to study the movements of the victims, for example in case of stalking.

In other cases, these means are used to bring about crime actively, through the diffusion of malwares or denial-of-service attacks, with the objective to damage an IT system. A malware is a program, apparently innocuous, downloaded unknowingly by an individual, with the aim to cause harm like network malfunctions, subtraction of information, unauthorized access to systems; it is commonly known as virus. Denial-of-service attacks have the intent of disrupting a website's functionality.

Notwithstanding these sophisticated techniques, ICTs are also used by the world to face and combat crimes, traditional and cyber ones. A perfect example is the use of bugs for wiretapping, through the "trojan horse" malware. Video cameras, artificial intelligence, and regular update of credentials and passwords, are other examples of devices and techniques to counter the so-called cybercriminals.

The main problem is the compliance of these instruments with the traditional physiognomy of guarantees provided for by legal systems. Despite all rules of law in force, written or not, being actualized in respect to press, IT document, and in part also videocameras, today the compatibility of these new means with disciplines is discussed a lot, both in jurisprudence and by scholars. Indeed, it is necessary to reason about the legislative void caused by these advanced technological products, in order not to lose the opportunity to guarantee efficacy and efficiency to systems, but also without oppressing the right to a fair and equal trial. The more appropriate solution in this case is a joint reading of disciplines, opting for the balancing method[3]. Nevertheless, although there is an open diatribe on this matter, laws that regulate information and communication technologies turn out to be inadequate, if not obsolete, nowadays, because they are founded mostly on the idea of a physical and territorial space, which cyberspace is not. ICTs operate in an indefinite space, which does not consider neither physical borders nor geographical ones. For this reason, cyberspace is called borderless, without boundaries, typical characteristic linked to limitlessness and immateriality.

[3] J. KLEIJSSEN, P. PERRI, *Cybercrime, Evidence and Territoriality: Issues and Options*, Netherlands Yearbook of International Law, Springer, 2017

Indeed, in this scenario, communities are not localizable precisely anymore: they do not belong to a specific place, therefore violating ordinary principles of space and time[4], and expanding unlimitedly and in a figurative way to global territories. Not by chance, cyberspace has been called also Fifth Domain, after air, land, sea and space[5].

In other words, it is the virtual dimension where users, connected among each other through networks, can move and interact in order to pursue different purposes and objectives. Italian Strategic Framework for the Security of cyberspace (*Quadro Strategico Nazionale per la Sicurezza dello spazio cibernetico*) has tried to define this concept as "set of interconnected information technology infrastructures, comprehending hardware, software, data and users, as well as logic relations, established among them"[6].

It is a work of man, and for this reason it is susceptible of constant evolutions, structural and functional ones. In order to explain the web structure, scholars make use of the iceberg shape, to properly underline the difference between what is clear and accessible (tip), and what is hidden (depth). The tip of this iceberg, the visible part, is the so-called Clearnet, the portion of Internet accessible to everyone through search engines and browsers like Google; then, there is the Deep Web, sites present in networks, but not indexed by search engines: for instance, it refers to Intranet websites, designated for a narrow circle of people, like private corporate sites. Dark Net consists in virtual networks, navigatable anonymously and using the appropriate systems protected by passwords. And finally, Dark Web, the most obscure and hidden part of the iceberg, accessible only through dark net, mainly to conduct illicit activities. In the last few years, users who enter into contact with Dark Web reality are a lot, especially to carry out money exchanges with bitcoins, or sale of personal and reserved data[7].

---

[4] A.C. AMATO MANGIAMELI, *Diritto e Cyberspace: appunti di informatica giuridica e filosofia del diritto*, «Infatti, nel cyberspazio, le comunità non sono più localizzabili con precisione; non hanno più un luogo, violando così i principi dello spazio e del tempo ordinari»

[5] M. MIRTI, *La disciplina giuridica del cyberspace*, www.opiniojuris.it, 2016

[6] "L'insieme di infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati e utenti, nonché relazioni logiche, comunque stabilite tra essi" (Quadro Strategico Nazionale per la Sicurezza dello spazio cibernetico)

[7] See *The Clearnet, the Deep Web and the Dark Web*, www.osinttraining.net

In general, cyberspace is not exactly what it seems, it hides obscure realities, not accessible to everyone, but mostly it gathers great amounts of data, both legal and not. The aforementioned data may constitute the so-called Big Data. The latter corresponds to the complex of activities for the elaboration and management of information acquired and handled by societies and entities. They are produced directly by people, with the act of registering to a social network, or to a digital platform, and stored by ICT (Big Data Management). Through this data, information on users is extracted, to suggest (prescriptive analytics) or predict future actions (predictive analytics). Big Data Analytics are so important because they help to simplify corporate movements, to make more efficient decisions, to increase profits and have satisfied clients[8].

Despite "Big Data" references being widespread in the last few years, this concept is actually in force since the end of the Nineties and the beginning of the Two-Thousands, thanks to the analyst Doug Laney, who formulated the "Three Vs Model", about the three main characteristics of Big Data, which are: Volume, because the massive amount of data derives from different sources such as social media or online transactions; Velocity, property of data transmission itself, in real time; Variety, referring to the uneven nature of this information, contained in photos, documents, videos or audios[9]. Over time, this theory has been studied and analyzed, up to be implemented into the "Five Vs Model", including two new concepts: Veracity, which is reliability of data, and Value, so the importance of it[10].

Big Data has entered in everyday life of people, through personalized marketing, memorization of habits, localization, but it is also used for public interest causes, for instance in case of political elections with surveys.

On the one hand, today people fear this excessive control by ICTs, able to formulate algorithms on the basis of what has been read, looked or even said, on the other hand Big Data Analytics has permitted to strengthen cyber-defenses, improving cybersecurity. These elements may help to track down suspicious and anomalous activities, typical of phishing, or to strengthen IT security measures with constant

[8] See *Big Data*, www.blog.osservatori.net

[9] R. KITCHIN, G. MCARDLE, *What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets*, Big Data & Society, 2016

[10] D. S. SINGH, G. SINGH, *Big Data – A Review*, International Research Journal of Engineering and Technology, volume 4, Apr 2017

updates or data cleaning, thus giving the possibility to prepare different types of defense strategies. Together with Big Data, a relevant position within the entire framework related to cyberspace has been acquired by Artificial Intelligence and Machine Learning. These are instruments used to learn and replicate human thinking automatically. AI and ML can be used both with good intent, trying to innovate and improve cybersecurity, and to perpetrate more sophisticated information technology attacks. Indeed, cybercriminals often use artificial intelligence as an assault method, because it may facilitate reaching objectives faster: for instance, there are already a lot of systems based on AI, which may guess passwords or spread malwares via email. Machine Learning and Artificial Intelligence learn from their mistakes and improve strategies step by step for new attacks[11].

If on the one hand improper and illegal use of these instruments is spread a lot, on the other hand artificial intelligence is used by cybersecurity to detect threats, to defend from IT assaults and hacker presence. Algorithms identify these aggressions and consequently undertake targeted actions.

Notwithstanding cybersecurity is a good starting point, both as preventive measures (which try to reduce commission of crime) and protection measures (to mitigate seriousness of damage), safety within cyberspace is still far. Because of its constant evolution, brand-new types of offences arise, together with new techniques of consummation of crime: new modalities of defamation, racism, revenge porn are just some of the crimes widespread in recent times, belonging to the cybercrime category.

1.2 CYBERCRIME: DEFINITIONS AND MANIFESTATIONS

Cybercrime is one of the most dynamic typologies of offence in the world, since it is the direct consequence of technological progress, constantly evolving. It is a serious phenomenon that consists in the commission of illicit activities aiming to damage information and communication technologies or using them to consume

[11] D. GREENE, A.L. HOFFMANN, L. STARK, *Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning*, www.aisel.aisnet.org, 2019

the crime, in a cross-border dimension. Despite there not being an approved definition by international society, certainly it can be said that the use of IT instruments is essential in order to integrate this offence.

Cybercrime is none other than the evolution of criminality to the present day, with modern means. It slips away from traditional models, characterized by legal systems, for the lack of geographical boundaries and mostly for its transnational characterization[12]. Indeed, globalization has permitted the creation of a borderless cyberspace: threats are valid for all States of the world, and its transnational nature allows connections among individuals, regardless of the place.

Cybercriminals' identity is basically unknown and difficult to discover, because it is concealed by anonymity most of the times. Nevertheless, scholars have supposed that generally, it may concern male individuals, located in developing countries, aged between 18 and 30 years old. Their purpose is to identify weaknesses of systems and IT instruments, taking advantage of them and manipulating, cancelling or stealing information. Reasons to make these practices are different: someone acts for profit-making causes, others for terrorism, others even for personal reasons, like revenge. Therefore, intent is certainly one of the main features of this offence, related to the concept of *mens rea*.

It hardly ever happens that cybercriminals act alone. Some organizations and entities, like UNODC, INTERPOL and EUROPOL, estimated that these subjects perpetrate their conducts in group, or in association, in order to achieve their aims easily[13]. This phenomenon constitutes a true manifestation of organized crime, in which cyberspace is the action field.

Cybercriminals may perform different roles: among those who conduct stable functions, there are coders, individuals responsible for developing malware and other tools to commit cybercrime; hackers, individuals responsible for exploiting the vulnerabilities of systems, networks and applications[14]; technicians, individuals responsible for the technical support of operations, keeping instruments available.

[12] A. MATTARELLA, *La futura convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, Sistema Penale, 2022

[13] INTERPOL, *Global Cybercrime Strategy*, 2017

[14] UNODC, *Digest of cyber organized crime*, Vienna, 2016

Besides that, there are also subjects who conduct temporary functions, on the basis of the necessities of the organization.

Essential condition is the respect of all organized crime parameters, so a minimum of three people, with a permanent bond and with the purpose of realizing an undetermined program of crime. The members of these organizations could not be in the same geographical place, but they may collaborate online: indeed, a special peculiarity of this type of offence is de-centralization. These individuals, covered by anonymity, use forums and digital platforms to communicate among each other and study the movements of their victims. Cybercriminal groups can be distinguished into three categories: the one which operates mostly online and commits cybercrime in the strict sense; the one that operates both online and offline, perpetrating crimes with different natures; and at last, the one which operates basically offline, but uses IT instruments to expand and facilitate activities.

In the first category, there are the so-called swarms and hubs. Swarms are groups of people who conduct activities ascribable to cybercrime, mostly for ideological purposes, and for a certain period of time. Once their objective is achieved, these groups disband. Hubs consist in a more structured and organized group of individuals, who perpetrate typical actions such as phishing, malware and DDoS diffusion etc. These operations are profit-driven.

The second category is composed of hybrid groups: both online and offline activities are conducted, like identity theft and frauds. These operations are profit-driven too.

The third category includes associated individuals, who operate mainly offline: the use of ICTs is marginal, reserved to facilitate and improve off-net activities[15].

Cybercrime phenomenon has a lot of characteristics, recurring in every manifestation or expression: as it was said, evolution is an intrinsic element of this type of offence, deriving from the constant development of information and communication technologies. Hence, the phenomenon is continuously changing, together with its modalities.

Another element already mentioned is the absence of borders, as well as transnationality, but referred, in this case, to the range of action of the crime,

[15] UNODC, *Digest of cyber organized crime*, Vienna, 2016

characteristic originated from the concept of cyberspace: indeed, it is not necessary that the author would be in the same geographical place of the victim for conducting the computer assault: everyone may be subjected to cybercrime, because there is one and only cyberspace.

In accordance, another peculiarity is the difficulty to localize cybercriminals. The latter might be anywhere in the world, reason why for the authorities it is complicated to identify the exact point from which the IT attack has started.

The fourth fundamental characteristic: cyber-action is silent, so it is difficult for victims to realize what they are suffering in a short time. It happens perhaps during a program download, which downloads a virus automatically, or in case of phishing, with e-mails whose aspect looks like the official counterpart.

Most of the times, victims become aware of the damage after the crime has been implemented, because of the lack of "physicality" of the attack. Indeed, often a serious or material damage does not occur, but this does not exclude the constitution of the offence.

Last and fifth peculiarity is anonymity: typical on the Internet, essential for people who perform crime and act undisturbedly, without being identified quickly. Basically, cybercriminals use TOR software, The Onion Router, which allows anonymous conversations. Thanks to this mean, authorities have a lot of difficulties to track illegal operations and users, conducted within the Dark Web.

These characteristics are contemplated in all typologies of cybercrime, in spite of the different expressions in cyber-dependent ones and cyber-enabled ones.

Cyber-dependent crimes are those criminal conducts which necessitate of a technological support, without which it would not be possible to perpetrate an offence included into this category. It contemplates as object and legally protected right, reserved access, integrity and protection of data and systems. Some of these crimes are: illegal access or hacker attacks, illegal interception or acquisition, data and system interference, misuse of devices[16].

Illegal access means unauthorized access into an ICT, through which data is generally hacked. It is the prerequisite of each other information technology attack. Hacker assaults consist not only in obtaining access illegally or without

[16] P.N. GRABOSKY, *Cybercrime*, Oxford University Press, 2016

authorization, but also the excess of powers after a conferred permission. For the configuration of this type of crime, violation of protection measures is necessary, which may endanger the privacy of data and information. Once the conduct has been brought about, remotely or locally, it would be possible for criminals to download, alter, steal or damage systems, or even disable the access to legitimate users.

Direct consequence of this offence is illegal interception or acquisition. It does not have a specific definition, but the most used is the one provided for by the Budapest Convention on cybercrime, "interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electro-magnetic emissions from a computer system carrying such computer data"[17]. In general, this offence consists in holding information obtained after an illegal access.

Data and system interference concern all those activities which alter, cancel or inhibit data functioning, damaging their integrity. It presupposes an illegal access. In this type of crimes, mainly malicious software (or malwares) is used, with the aim to cause widespread damage, such as disturbance and malfunction of networks, subtraction of information and unauthorized access to systems. One of the most known and used malwares is ransomware, which infect a device, making its data inaccessible and requesting a ransom to pay to unlock it[18]. To spread it, cybercriminals use phishing e-mails, that invite the victim to open links or download infected files.

Another type of attack could be perpetrated through the Distributed Denial of Service, also called DDoS, with the purpose of making a website or an online service useless, overloading it with access requests and spam originated by different sources[19]. In order to achieve their intent, crime authors use the so-called Botnet, a set of computers compromised by malwares, which permit to take control of instruments.

And finally, the last typology of cyber-dependent crime, that is the misuse of devices: it is considered illegal when it is committed without having the right, and

[17] Art.3, Chapter II, Council of Europe Convention on Cybercrime, Budapest, 2001
[18] See *What is a Ransomware*, www.kaspersky.com
[19] See *DDos*, www.malwarebytes.com

intentionally. This offence provides for possession, production, sale, distribution of devices, including computer programs. The misuse of them regards also passwords and access code, which may consent illegal access or interference.

Cyber-enabled crimes concern traditional offences, characterized by legal systems, and committed by authors with the use of ICTs. In this category, technology has an accessory and secondary role: crimes could be conducted offline, but they are enhanced by the use of computers, networks or other forms of information and communication technology. In some cases, they facilitate the commission of a crime; in other ones, these instruments can be used to expand the effects[20].

As compared to cyber-dependent ones, cyber-enabled crimes vary with the different juridical goods and legally rights protected: economic-related cybercrime and online marketplaces for illegal items protect people's assets and property interests; malicious and offensive communications including cyber-bullying, xenophobia and racism and offences against specific targets like cyber-stalking and revenge porn protect psychophysical integrity and dignity of individuals; child sexual offences and indecent images of children including child sexual abuse and exploitation, online grooming and child pornography protect the mental balance, psycho-sexual integrity and freedom of children .

Economic-related cybercrimes are those offences providing the use of computer systems with the objective to cause an unfair financial loss to the victim and an advantage to the author. Not always victims report these actions; in the majority of cases because they do not notice the infraction immediately, or in other cases to avoid reputational damage, especially for corporations. Within this category of crime, the most important one is certainly fraud: hiding behind anonymity, authors conduct actions willingly and unrightfully, which cause loss of property by an individual, after an input of alteration, cancellation or suppression of data. This offence involves the use of false information in order to obtain something by a specific and designated target.

Within fraud category, the most common crimes are the bank ones, fraudulent sales with online auctions or fake e-commerce websites, and obviously phishing: criminals, pretending to be a reliable entity, use apparently legitimate but false e-

[20] UNODC, *Global Programme on Cybercrime*, www.unodc.org

mails, requesting for passwords or bank account data. In this way, they mislead victims, who suffer great financial losses[21].

Phishing belongs also to that section of crimes perpetrated via Internet which include someone's identity theft, illicitly assumed by another one[22]: other offences belonging to this category are Bin Raiding, so looking through rubbish for bills or other paper containing confidential information; Skimming, stealing credit or debit card numbers by using a special device when processing cards; Changing Address, sending someone's billing statements to another location; Pretexting, fraudulently gaining access to personal information from financial institutions, telephone companies and other sources.

Another type of computer fraud, which is becoming increasingly popular in recent years, is fake online love stories through social network and dating apps. Authors enter victim's life gradually, establishing a trustful relation that gives rise to a pseudo-love story. Once the victim is persuaded, they are instigated to show and bestow personal information or money.

Intellectual property crimes belong to cyber-enabled ones: intellectual property is considered for all intents and purposes a real right, protected by copyright. Offences against it generally consist unauthorized use or sale of the patent. Within this category, the more popular crime is piracy, that is unauthorized copies of video or audio registrations, for profit purposes. Internet is the more spread mean to distribute, share or make music, films and other pirated products available through streaming services, for instance.

Counterfeiting occurs when money or goods are counterfeited, sold on the Internet and invoiced as authentic, for profit purposes.

Counterfeiting is different from forgery, which implies fabrication of fake documents with false personal information, misleading people. It may have as object passports and forged ID.

---

[21] S. DOWLING, M. MCGUIRE, *Cybercrime, a review of the evidence: Research report 75*, www.assets.publishing.service.gov.uk, 2013

[22] R. FLOR, *Phishing, Identity theft e identity abuse: Le prospettive applicative del diritto penale vigente*, Rivista italiana di diritto e procedura penale, 2007

Online Marketplaces for Illegal Items are used by criminals not only to exchange IT techniques and instruments, but also for illegal trafficking, like drugs, firearms or people. This marketplace lives in the dark web, safe space for such activities.

Despite the two Additional Protocols of UN Convention on Transnational Organized Crime (UNTOC) providing a specific protection for these conducts, by now trafficking of persons and smuggling of migrants belong to cyber-enabled crime. In this case, ICTs are used by criminals to facilitate and promote contraband practices.

All of these crimes mentioned till now, predominantly with economic and profit-driven purposes, have money laundering as conclusion of the entire criminal conduct. To ensure that money results "clean", criminals employ illicit profits into licit activities. In the last few years this practice has been implemented also in its cyber modality, the so-called cyber-laundering, concealing through network and new systems of payment.

Since the creation of social networks like Facebook, Instagram etc., offensive and threatening messages are commonplace, especially among young people.

Cyber-bullying or trolling include mockeries using information technologies like chats, apps and others. They are supervised and checked by authorities because they constitute one of the main causes which bring young people to suicide, in growing trend, together with specific types of bullying such as body-shaming and homophobia.

As it has been said before, cyber-enabled crimes contemplate criminals using ICTs for ancillary purposes, to facilitate consummation of offences or to study the victim's movements, like in the case of cyberstalking and computer harassment.

Records show that the majority of victims are females, who suffer of online bothering activities or violence.

Cyberstalking consists in threatening conducts and not-desired attentions through an IT instrument; generally, these practices are tied to traditional ones, like tailing or making undesired phone-calls.

A brand-new crime, born following the ICTs' evolution, is revenge pornography, known simply as revenge porn, which consists in the publication or threat of sharing photos or videos illustrating a person involved in sexual activities: private

documents generally not shown to public. This offence interests mainly couples or former ones, with the purpose to cause humiliation and embarrassment to the victim, as a revenge for breaking up or cheating[23].

Among all cyber-enabled crime, the most serious one is without any doubt child sexual offences and indecent images of children.

The predators, mainly adults, intercept children and young people, through, among others, Internet websites (online grooming), establishing fake relations of trust with them. Often, these adults are people already known by the minor, such as a relative or an educator. Therefore, the fraudulent, pervert and manipulating mind of the author is opposed to the innocence and weakness of children. They are abused and exploited, persuaded to conduct sexual activities, alone or with other people, while being recorded. Children become sexual toys to fulfil adults' fantasies. Another related crime is diffusion of this type of materials, an easy practice for ICTs, especially in the Dark Web, chat and e-mails.

The real problem consists in the devastating consequences of these activities on children: the latter would live constantly in disturbed psychological conditions, causing these young people to receive an often permanent scar to their self-esteem, bringing them to feelings of shame. Very often child sexual abuse and exploitation are a prelude to suicide tendencies.

Even though the majority of organizations and institutions talk about only of two categories of cybercrime, cyber-dependent one and cyber-enabled one, at present several scholars prefer a tripartition of digital criminality in crime against machine, such as hacking and DDos attacks, crime using the machine or computer-assisted crime like piracy, robberies and scams, and finally crime in the machine, also known as computer-content crime, for instance online hate, harassment, pornography. This classification was adopted also by the European Commission. Instead, other scholars classify true cybercrime, where the computer is the target and the crime could not occur without a computer; hybrid crimes where the computer plays a role, but the crime could still be committed without the involvement of computer; cyber-assisted crimes, where the computer's

[23] OSSERVATORIO CYBERSECURITY EURISPES, *Non consensual pornography: dal revenge porn alla sexual extortion*, Studio Legale De Vita, 2019

involvement is incidental to a real-world crime, and simply increases the opportunity for traditional crimes[24].

In accordance with assessments and statistics conducted by States and international organizations on the incisiveness of cybercrime in the world, hacker attacks perpetrated against governments and critical infrastructure are the most carried out by cybercriminals, to be followed by cyber-attacks against cybersecurity measures, trying to weaken them. Cyber-enabled crimes like phishing, fraud, identity theft and child sexual abuse are strongly increasing, endangering mostly people's image and the economic sector[25].

1.3 THE PROPULSIVE ROLE OF THE UNITED NATIONS IN THE INTERNATIONAL FRAMEWORK AND IN THE FIGHT AGAINST CRIME

The United Nations is an international organization founded in 1945. Currently made up of 193 Member States, the UN and its work are guided by several disciplines contained in its founding Charter, considered a treaty-constitution[26], because it is composed of rules on the purposes of the organization, its general principles to which it should aspire, but also fundamental rights and duties of Member States.

The purposes of the United Nations, indicated in the article 1 of the Charter, are "to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace; to develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace; to achieve international co-operation in solving international problems of an

[24] K. PHILLIPS, J.C. DAVIDSON, R.R. FARR, C. BURKHARDT, S. CANEPPELE, M.P. AIKEN, *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, Forensic Sci, 2022

[25] See "Rapporto Clusit 2022"

[26] S. MARCHISIO, *L'ONU: il diritto delle Nazioni Unite,* Il Mulino, Bologna, 2000

economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and to be a centre for harmonizing the actions of nations in the attainment of these common ends"[27].

The expanse of these purposes explains how broad are the actions, and in general the work of the United Nations, involving sectors of different natures: development, protection of human rights and fundamental freedoms, crime prevention, peace-keeping, international collaboration and so on.

In order to implement the UN Charter, Member States must follow specific principles indicated in the article 2[28]: the principle of the sovereign equality of Member States; good faith of the obligation of sincere cooperation; duty of peaceful settlement of disputes; refraining from the threat or use of force against the territorial integrity or political independence of any state; providing assistance to Member States; the maintenance of international peace and security.

"Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter"[29].

The principle of the sovereign equality is the premise on which all international relations are founded. Each Member State enjoys the same rights and duties, and they are equal members of the international community, despite differences related to economic, social, political fields or others. Sovereign equality means that States are juridically equal, and they must respect the legal personality of the other ones: territorial integrity and political independence are inviolable[30].

The affirmation of the principle of sovereign equality includes also the principle of non-discrimination, recalling the paragraph 3 of the article 1 of the Charter on the purposes of the UN, and in general the prohibition of any kind of discriminations, including also those referring to different conditions and circumstances of States.

[27] Art.1 of the Charter of the United Nations
[28] Art.2 of the Charter of the United Nations
[29] Art. 2, paragraph 7 of the Charter of the United Nations
[30] M. MUGNAINI, *ONU: una storia globale*, Franco Angeli, 2021

According to the paragraph 2 of the article 2 of the aforementioned Charter, Member States must fulfill in good faith the obligations assumed, in order to ensure the rights and benefits resulting from their membership. The principle of good faith is a general duty of Member States of fairness and integrity in mutual relations and also towards the organization, to guarantee that each State may gain advantages from the membership to the United Nations.

This second paragraph is connected to the fifth one of the same disposition, according to which Member States "shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action"[31]. The obligation of assistance constitutes a duty of general content, by which all Member States are owners towards the organization, to perform the services that contribute to implement the purposes of the UN.

The third paragraph of the article 2 recalls the obligation for UN Member States to resolve their disputes by peaceful means, so that peace and justice are not endangered.

And finally, the paragraph 4 of the same article discipline that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations". The use of force is forbidden, together with the war obviously, and also the simple threat of it: Member States are deprived of the so-called *ius ad bellum*[32].

The main organ which bring about the functions and powers of the United Nations is the General Assembly. The membership is directly attributed to all the Members of the UN[33], as it is provided for by the article 9 of the Charter, and it is the only body in plenary composition. The General Assembly may discuss any questions or matters within the scope, or relating to the powers and functions of any organs, and may make recommendations to the Members of the United Nations or to the Security Council or to both on any such questions or matters[34].

---

[31] Art.2, paragraph 5 of the Charter of the United Nations
[32] S. MARCHISIO, *L'ONU: il diritto delle Nazioni Unite,* Il Mulino, Bologna, 2000
[33] Art.9 of the Charter of the United Nations
[34] Art.10 of the Charter of the United Nations

The rights provided for by the Charter to the General Assembly are brought about by the single delegates of each Member State, expressing the voting right with the *consensus*.

Participation in the work of the General Assembly sometimes requires a large number of representatives supported by consultants and experts to carry out the debates and participate in the final deliberations, the results of negotiations carried out in the framework of committees, working groups meeting formally and informally. The power to create subsidiary bodies is provided for by the article 22 of the Charter, pursuing the fulfillment the purposes of the United Nations[35]. These organs have specific competences, related to the reason why they were created.

The General Assembly has established a very large number of subsidiary bodies including study committees, political commissions, administrative assistance bodies, operational agencies and judicial bodies. Indeed, also implementing article 13, the General Assembly has the task of undertaking studies and making recommendations in order to encourage the progressive development of international law and its codification[36].

The representation of single Member States at the United Nations is constituted by physical persons, legitimated to participate as delegates, and belonging to the General Assembly.

Delegates belong to the so-called Permanent Missions, whose functions are representing the State at the organization, maintaining relations among them, leading negotiations.

Besides the member status, another role which can be identified within the composition of the General Assembly is the Observer status. It belongs to international organizations such as the European Union, but also other entities like Holy See. Observers participate actively to the General Assembly's meetings, having the floor to express their opinions on the matter analyzed.

The acts which are delivered by the United Nations are several: one of the most common is the recommendation. It is not binding, but States should follow the content, in accordance with the article 2 of the Charter. Decisions are binding acts,

[35] Art.22 of the Charter of the United Nations
[36] Art.13 of the Charter of the United Nations

generally delivered for the approval of financial reports, or for security measures. The resolutions are the most important acts that the United Nations can adopt: they are formal expressions of the opinion or will of UN organs. Since its formation, the United Nations cares about issues related to the economic and social development, especially because of a world strongly characterized by inequality in many sectors. The multilateral cooperation, that States pursue through international organizations with a universal nature such as the United Nations, find their legal basis in the founding treaties of these organizations and in the resolutions adopted. In order to reach a functional economic and social cooperation, the United Nations can establish specialized agencies in economic, social, cultural, educational, health and related fields, according to the article 57 of the Charter[37]. In addition, it was established also the Economic and Social Council, also known as ECOSOC, whose functions are indicated in the article 62: it "may make or initiate studies and reports with respect to international economic, social, cultural, educational, health, and related matters and may make recommendations with respect to any such matters to the General Assembly to the Members of the United Nations, and to the specialized agencies concerned. It may make recommendations for the purpose of promoting respect for, and observance of, human rights and fundamental freedoms for all. It may prepare draft conventions for submission to the General Assembly, with respect to matters falling within its competence. It may call, in accordance with the rules prescribed by the United Nations, international conferences on matters falling within its competence"[38].

In accordance with article 63, ECOSOC can conclude agreements with the agencies referred in article 57, and coordinate their activities through consultations and recommendations[39].

And finally, according the article 71, the Economic and Social Council "may make suitable arrangements for consultation with non-governmental organizations which are concerned with matters within its competence. Such arrangements may be made with international organizations and, where appropriate, with national organizations

[37] Art.57 of the Charter of the United Nations
[38] Art.62 of the Charter of the United Nations
[39] Art.63 of the Charter of the United Nations

after consultation with the Member of the United Nations concerned"[40]. In carrying out its mandate, ECOSOC consults with representatives of academia, private sectors and with those non-governmental organizations which have obtained consultative status from it[41].

In the international framework, the United Nations is not a global government, but it provides means which can assist the resolution of international conflicts, peace-keeping, the development of friendly relations and cooperation among States and also the formulation of policies on questions of common interest[42].

Through its agencies, the UN can develop various projects regarding matters of any nature, bringing to light issues that in the past were not even considered. The creation of specific groups of work and committees has allowed to analyze themes, leading to significant steps forward at universal level.

Indeed, in order to enhance as much as possible the current global situation, the United Nations provides a shared blueprint for peace and prosperity for people and the planet, called 2030 Agenda for Sustainable Development[43]. This program includes seventeen sustainable development goals which represent common purposes on a set of questions important for development. This means that all States and individuals are concerned: nobody excluded and left behind. Among these seventeen goals, some of them are "no poverty", "zero hunger", "gender equality", "reduce inequalities", and guarantee "peace, justice and strong institutions". In reference to the latter, which is the sixteenth SDG, it is necessary to promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels[44].

Prevention and fight against criminality are part of this goal, although it is an UN's purpose since always, by facing crime of each nature. Indeed, even before the creation of the 2030 Agenda, the United Nations established many groups of work

[40] Art.71 of the Charter of the United Nations
[41] ECOSOC Resolution 1996/31: Consultative relationship between the United Nations and non-governmental organizations
[42] B. CONFORTI, C. FOCARELLI, *Le Nazioni Unite*, Cedam, 2020
[43] See https://sgds.un.org
[44] See https://sdgs.un.org/goals/goal16

specialized on certain offences, but above all the Commission on Crime Prevention and Criminal Justice.

The Commission on Crime Prevention and Criminal Justice (CCPCJ) was established by the Economic and Social Council resolution 1992/1[45], upon request of General Assembly resolution 46/152[46], as one of its functional commissions.

The Council has established the Commission's mandates and priorities, which include international action to combat national and transnational crime, including organized crime, economic crime and money laundering; promoting the role of criminal law in protecting the environment; crime prevention in urban areas, including juvenile crime and violence; and improving the efficiency and fairness of criminal justice administration systems (resolution 1992/22[47]).

The Commission guides the activities of the United Nations in the field of crime prevention and criminal justice. It also reviews United Nations standards and norms in this area, including their use and application by Member States. It takes action through resolutions and decisions.

The CCPCJ also offers Member States a forum for exchanging expertise, experience and information in order to develop national and international strategies, and to identify priorities for combating crime.

In 2006 the General Assembly adopted the resolution 61/252[48] which further expanded the mandates of the Commission on Crime Prevention and Criminal Justice to enable it to function as a governing body of the United Nations Office on Drugs and Crime (UNODC), and to approve the budget of the United Nations Crime Prevention and Criminal Justice Fund.

The CCPCJ holds annual regular sessions as well as intersessional meetings, to provide political guidance to UNODC. Toward the end of each year, the

[45] ECOSOC Resolution 1992/1: Establishment of the Commission on Crime Prevention and Criminal Justice

[46] General Assembly Resolution 46/152: Creation of an effective United Nations crime prevention and criminal justice programme

[47] ECOSOC Resolution 1992/22: Implementation of General Assembly Resolution 46/152 concerning operational activities and coordination in the field of crime prevention and criminal justice

[48] General Assembly Resolution 61/252: Questions relating to the programme budget for the biennium 2006-2007, paragraph XI "Strengthening the UN Crime Prevention and Criminal Justice Programme and the role of the Commission of Crime Prevention and Criminal Justice as its governing body"

Commission meets in a reconvened session to examine budgetary and administrative matters such as the governing body of the United Nations Crime Prevention and Criminal Justice Programme.
The collaboration between the CCPCJ and UNODC stems from the fact that these two UN organs have the same purpose and scope: crime prevention, criminal justice, fight against criminality.
Even about cybercrime, the Commission has given its contribution establishing an open-ended intergovernmental expert group to conduct a comprehensive study on cybercrime.
Since its appearance, this offence has been considered a dangerous and though phenomenon by this organization, reason why it was monitored also through recommendations and resolutions, which will be analyzed in the next paragraph.

1.4 HISTORICAL OVERVIEW OF EXISTING INSTRUMENTS

The necessity to discipline those conducts belonging to the cybercrime category at international level arises from the will of States of the world to promote attempts of regulation of this type of offences, and in general of this new expression of criminality. For a long time, these crimes remained unpunished, or condemned with non-proportionated sanctions, because of the lack of legislations.
Only in 1976, some steps forward were made. Precisely in that year, the First Conference of the Council of Europe was held in Strasburg, which concerned about illicit conducts committed with information and communication devices, in a very mild and generic way.
In the following years, slowly, a lot of organizations treated the matter, and among them also the Organization for Economic Cooperation and Development which deals with the analysis of the impacts deriving from politics in order to guarantee socio-economical wealth. In 1986, OECD examined disciplines on crime and abuses perpetrated with information technologies through some recommendations in depth, more specifically about electronic frauds, forgery, damaging of software, violation of programs and processors, unauthorized access.
In 1989, the Council of Europe defined this phenomenon in detail, drawing up two lists: the “minimum list”, providing criminal conducts that European States should

prosecute (such as computer fraud, forgery, unauthorized access to systems, damage of data and programs etc.), and the "facultative list", in which conducts deemed not-excessively offensive are included, requiring a juridical action by national judges (unauthorized alteration of data, divulgation of information covered by professional secret).

These recommendations produced by the aforementioned organizations analyzed criminal phenomena related to cyber-dimension only in its substantial side. Nothing was said about the procedural aspect. For this reason, in subsequent years, the Council of Europe, through another recommendation, focused entirely on cybercrime, including also the procedural point of view.

In 1994, the United Nations created the Manual on the Prevention and Control of computer-related crime[49], a non-binding document containing disciplines on the misuse of information technologies. It could be considered the true implementation of the General Assembly Resolution 46/152 and ECOSOC Resolution 1992/22 about the programme on prevention of crime, in this specific case related to the digital dimension. The Manual is focused on the transnational nature of computer-related crimes, underlining the constant evolution to which they are subjected. The purpose of this guide is to assist in developing a common framework for understanding the implications of computer-related crime for the entire world. As it was said, it is not binding, but Member States may use it to better understand the problem, to become aware of some solutions that have been recommended, to develop their own response and to foster international cooperation, solution to counter a transnational offence.

Between 2000 and 2001, the United Nations General Assembly formulated also two resolutions on the integrity of data principle and on the adequate education that technicians should have about cyberspace, using ICTs for positive purposes.

All the juridical acts mentioned are soft law ones, without a real incisiveness in domestic law. Only in 2001 it was drafted the very first Convention on cybercrime, the Budapest Convention[50].

[49] United Nations Manual on the Prevention and Control of Computer-Related Crime, New York, 1994

[50] The Council of Europe Convention on Cybercrime, Budapest, 2001

It was signed up by the Council of Europe and has 66 States of the world participating, both members of the council and not: indeed, some signatories are Canada, Japan, South Africa and United States of America. This was possible because the real reason which has brought to the redaction of this convention is the dangerousness of the international nature of cybercrime.

Therefore, this legislation underlined the necessity to harmonize regulations belonging to different countries, trying to uniform law and counter a widespread phenomenon, especially through international collaboration.

The Budapest Convention was formulated in order to establish a guide for each state which wants to elaborate a complete system of rules to combat cybercrime, as well as creating a framework on cooperative activities. The method used to draft this convention was not chosen by chance: in fact, conducts are settled instead of technologies, so granting the validity of laws and procedures during the course of the time.

The objectives which the Convention has tried to reach are: first and foremost, to criminalize violations of privacy, integrity and disposition of data and IT systems, infractions connected to information technology, and at last, those offences perpetrated through online contents, such as racist or xenophobic comments, or obscene images, like child-pornography[51].

In addition, this legislation establishes specific procedures to increase the efficiency of investigations, to provide for a juridical base for international cooperation among states, mostly on sharing information and mutual assistance.

The Budapest Convention is articulated in three sections: the very first articles analyze terminologies and crimes disciplined by the Convention itself, describing a series of conducts that must be necessarily punished by States; the second part faces matters related to the procedural aspect, while the final part is focused on international cooperation in a strict sense. According to this structure, article 1 of the Budapest Convention defines the glossary of the used terms, such as computer system, service provider, and most importantly, the notion of computer data: “any representation of facts, information or concepts in a form suitable for processing in

[51] See www.coe.int

a computer system, including a program suitable to cause a computer system to perform a function"[52].

From article 2, descriptions of modalities of illicit conducts come in succession, underlining some fundamental characteristics as fraud (intentionality) and action conducted without right (abusively and unauthorized).

It also highlighted the difference between cybercrime in a strict sense, or cyber-dependent ones, and cybercrime in the broad sense, or cyber-enabled ones: the first category consists in offences against security, integrity and functionality of data and IT systems. Indeed, definitions of illegal access, information technology damage, data and system interference, misuse of devices follow. The second category considers eventual cyber-offences, like electronic frauds.

From article 4 to article 22, methods of investigations are explained, in order to reduce information technology crimes effectively. More specifically, disciplines on judicial police roles are present, together with the protection of defensive guarantees within proceedings, pursuant the introduction of new technologies. At the core, the structure of the Convention lacks a discipline on electronic evidence.

From article 23 to article 35, the importance of cooperation among states is strongly stated, seen as the unique solution to contrast the transnational nature of cybercrime. For this reason, in these articles some general principles of international collaboration are indicated, for instance mutual assistance and recognition, as well as some practical instruments like extradition.

The results achieved by the Budapest Convention brought to improvements on cooperation and collaboration relations among States, and in particular among authorities. Education of judges, prosecutors and technicians on cybercrime has also been updated, to be in line with the times; investigation operations have been strengthened thanks to interventions by INTERPOL and EUROPOL.

One of the main objectives reached is the advancement and actualization of various measures to protect minors against online abuse and sexual exploitation, especially thanks to the joint legislation of the Budapest and the Lanzarote Conventions. Indeed, the Council of Europe formulated two other conventions with international

[52] Art.1 of the Council of Europe Convention on Cybercrime, Budapest, 2001

nature, together with the cybercrime one: Convention on the prevention of terrorism in 2005[53], and Lanzarote Convention in 2007[54]. The former provides for dispositions which identify conducts like enrollment and training of terrorists as crime, even perpetrated through Internet. It is the so-called cyberterrorism, or the convergence between terrorism and cyberspace: a set of illegal attacks using computers and networks to intimidate or assault governments and their populations[55]. The latter analyzes sexual exploitation and abuse of minors, also in an online environment. This convention has introduced the "grooming" concept, so soliciting children and young people through websites or social networks. The Lanzarote Convention led to the addition, in the Budapest Convention, of a section regarding sexual acts perpetrated by and with minors.

Besides the general discipline, the Council of Europe has also contemplated two additional protocols to the cybercrime convention. The First Additional Protocol, come into force in 2003, concerns racist and xenophobic acts, committed through information technology instruments: it extends the range of action of the convention to offences related to the spread of racism and xenophobia, providing the possibility of international cooperation to counter these types of phenomena. The protocol defines racist and xenophobic material as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors" (art.2 First Additional Protocol). This material is to be contained into the concept of computer data itself. Other conducts punished by the additional protocol are also IT dissemination of threats and insults with racist or xenophobic reasons, and justification of genocide (art.3-4-5-6 First Additional Protocol).

The Second Additional Protocol of the Budapest Convention concerns the enhanced cooperation and disclosure of electronic evidence. It "brings the Budapest

[53] The Council of Europe Convention on the Prevention of Terrorism, Warsaw, 2005

[54] The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 2007

[55] See www.cepol.europa.eu

Convention up to date with current, technological challenges", said the Secretary General Marija Pejcinovic Buric.

This Second Protocol, signed on May 12 2022, includes disciplines on direct collaboration with service providers for information on subscribers, cooperation between judicial authorities and individuals in case of emergency, but mostly, providing more protection of personal data[56].

Being able to respond to cybercrime threats constitutes a great step forward: it strengthens collaboration and judicial authorities' capacities of obtaining electronic evidence, giving a common law system for the divulgation of information among States Parties and trying to transcend territorial limits.

The real limitation of this convention is defined by the lack of worldwide inclusion: the so desired cooperation is thus reached by a restricted circle of nations.

Despite the Budapest Convention being the current most important legislation on cybercrime, also other organizations have made efforts for the writing of regulations about this specific type of offence, like the Organization of American States. Often indicated with the acronym OAS, it is a regional organization composed of 35 Member States, belonging to the Americas. The aim which it pursues is to guarantee peace and justice within states, in respect to principles of sovereignty and independence. Democracy, human rights, security and development are the foundation on which the organization is based.

In 1999, OAS established the Inter-American Cooperation Portal on Cyber-Crime and a Working Group on Cybercrime, which aim at strengthening international collaboration, promoting the exchange of ideas and information, and capacity building to counter the phenomenon. A method suggested by OAS is to educate and train prosecutors and judges on matters related to information technologies, for instance on electronic evidence or cybercrime charge. According to what "substantive cybercrime legislation" of this Inter-American Portal provides for, OAS Member States should also consider and make references to the Budapest Convention, carrying out principles and disciplines.

The previously mentioned Organization for Economic Cooperation and Development was one of the first international organizations to deal with security

[56] See www.coe.int

from IT attacks, mostly speaking about economic and social aspects, as well as technical ones, linked to law enforcement. In these last years, an objective pursued by OECD is to develop and promote policies encouraging the use of ICTs for positive purposes, supporting innovation and evolution. Reports made by the organization are many, especially on identity theft: moreover, OECD has elaborated some juridical acts, the so-called "recommendations" on digital security, analyzing all technological risks that may fall on corporations, and recommending some methods to weaken effects and consequences.

The European Union has turned out to be interested in cybercrime, especially after the emission of the Budapest Convention by the Council of Europe. In order to obtain coordination and harmonization of actions conducted by the Member States, the European Union has the objective to spread the knowledge of risks linked to cyber offences, and to improve capacities and competences of people, trying to reduce the intensity of these types of attacks as much as possible, both at European and domestic levels. Therefore, the European Commission established in 2004, the so-called ENISA, European Network and Information Security Agency, a platform which encourages exchange of information among European Union institutions, domestic authorities and private sector.

The most important document deserving attention is the Council Framework Decision 2005/222/JHA[57] on attacks against information systems, with the purpose to continue with projects started and conducted by the Budapest Convention. This decision is focused more on cybercrime in a strict sense, such as abusive access to systems and information technology damage: this act is complementary to the Convention, as they both aim to Member States cooperation.

Since the Lisbon Treaty[58] came into force, cybercrime has belonged to the category of crimes of the European Union's jurisdiction. This offence has obtained written rules of law, and not just jurisprudential interventions by the European Court of Justice. In detail, article 8 of TFEU underlines the importance of cooperation among Member States, especially to conduct joint operations to face crimes, with a wide

[57] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information system

[58] The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing European Community, signed at Lisbon, 13 December 2007

range of action. Article 83 of TFEU establishes European Union, particularly through its legislative bodies, the Parliament and the Council, may "establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis". These serious crimes are terrorism, trafficking in human beings and sexual exploitation, corruption, organized crime, cybercrime, money laundering.

The European framework on cyber-dimension also includes Regulation (EU) 2016/679[59] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the so-called GDPR), and the Directive (EU) 2016/1148[60] concerning measures for a high common level of security of network and information systems across the Union (the so-called NIS Directive). The latter plays a very important role, because it created a Cooperation Group, composed of representatives from the whole European Union, the Commission and ENISA, with the purpose to "equip" Member States with appropriate instruments to counter cyber-accidents. Together with the aforementioned framework, recently the European Parliament and Council have drafted the Regulation (EU) 2019/881, also known as "Cybersecurity Act"[61], on information and communications technology cybersecurity certification. It continues a path already paved, concerning security of networks, information and systems, and giving a common and uniform strategy to prevent and combat cyber-attacks. In order to achieve this objective, the regulation provided for a revision on the ENISA role. As said, originally ENISA had an assistance role towards Member States; thanks to the Cybersecurity Act, this agency has acquired a stronger value, aiding not only with technical guidance, but also supporting activities for Member States to handle the damage caused by information technology attacks.

[59] Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

[60] Directive (EU) 2016/1148 of the European Parliament and Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[61] Regulation (EU) 2019/881 of the European Parliament and Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification

With the introduction of a European system of certifications for information and communications technology for cybersecurity, this 2019 act has created a harmonized system of rules, aimed to discipline European schemes of cybersecurity certifications, in order to improve the functioning of the internal market, increasing security of IT instruments and networks within the European Union.

About the sanctioning system, the regulation consists Member States would establish their own laws on sanctions applicable in case of violations of European systems on cybersecurity certifications.

The Cybersecurity Act corresponds to an essential step forward in the legislative activity of European institutions about security of information and communication technologies. It tries to supply a common strategy on cybersecurity for all Member States, a purpose pursued both with a strengthening of the ENISA's role and with the introduction of a European system of certifications for information and communications technology for cybersecurity.

The latest act on this subject delivered by the European Union is the Commission Recommendation (EU) 2021/1086[62], whose aim concerns the identification of all necessary actions to coordinate EU efforts to prevent, counter and combat information technology attacks and their effects, responding through the Joint Cyber Unit: a set of joint operations coordinated by EU against IT assaults, supported also by ENISA and EUROPOL. Indeed, the European Police Office has established the EC3 (European Cybercrime Center), offering not only strategies to sustain investigations made by Member States, but also campaigns on cybercrime prevention.

A brand-new entity, created in these recent years, is acquiring a very incisive role is the European Public Prosecutor's Office (EPPO). It conducts investigative actions in the European territory, prosecuting crimes damaging European financial interests, indicated in the Directive on the fight against fraud to the Union's financial interests by means of criminal law (also known as PIF Directive[63]). As said, a lot of crimes like fraud, counterfeiting, forgery and so on have a cyber-dimension,

[62] Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit
[63] Directive (EU) 2017/1371 of the European Parliament and Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law

therefore even the European Public Prosecutor's Office oversees cyber-enabled crimes.

The Commonwealth of Independent States, composed of some former Soviet republics, adopted in 2001 an Agreement on Cooperation in Combating Crimes in the Field of Computer Information[64], also known as Minsk Agreement. It is focused on strengthening cooperation between Member States of the Commonwealth of Independent States to ensure effective prevention, detection, suppression, uncovering and investigation of offences related to ICTs.

Instead, in Asia, the Shanghai Cooperation Organization became widespread: it is an organization of eight Member States (also including India, China and Russian Federation), which in 2009 established the Agreement among the Governments of the SCO Member States on Cooperation in field of ensuring international information security[65]. It is focused on cybersecurity, providing common measures for coordination, development of instruments, a constant monitoring system and disciplines on protection from cybercrime.

Generally, people think that the more subjected states to this crime would be the more developed ones, with a lot of multinational corporations, for example United States of America or European Union Member States, but actually, states apparently less developed like Middle Eastern or African countries provided for *ad hoc* disciplines on cybercrime.

In 2010 the Arab League formulated the Arab Convention[66] on combating IT offences. This treaty has the main purpose to improve cooperation among Arab countries in the fight against crimes perpetrated through information and communication technologies, and in the protection of countries' interests. It also provides for general rules on ICTs, substantial and procedural provisions, and mechanisms for establishing a discipline on electronic evidence. The Arab

[64] Commonwealth of Independent States Agreement on Cooperation in Combating Crimes in the Field of Computer Information, Minsk, 1 June 2001

[65] Agreement between the governments of State Members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security of 16 June 2009

[66] Arab Convention on Combating Information Technology Offences, 21 December 2010, Cairo

Convention fulfils an important role in the international legal framework, mostly for its criminalization of cyber-terrorist attacks.

The Economic Community of West African States (ECOWAS) adopted in 2011 the "Directive on Fighting Cybercrime"[67] which prescribes offences related to ICTs such as fraudulent access, interference, data interception and data modification; the Southern African Development Community (SADC) created a Model Law on Computer Crime and Cybercrime[68]. Both of these documents were applied to a restricted circle of African States, respectively 16 and 15 countries.

Whereas, in 2014, the African Union, composed of 55 countries, drafted the Convention on cybersecurity and personal data protection[69]: it corresponds to a specific legislation dedicated to State Parties, providing a specific regulatory framework on these specific fields, linked to ICTs. The scope of this convention is to facilitate the interaction among institutions to promote cybersecurity, with a harmonized system containing mechanisms headed to combat cybercrime and privacy violations. Moreover, it encourages the development of new technologies and capacity building.

The African Union Convention uses parameters similar to the Budapest Convention's, especially about child-pornography and racist contents, considered crimes against humanity by the African Union.

The Commonwealth, organization among States previously belonging to the former British Empire, formulated in 2017 a "Model Law on Computer and Computer related crime" [70] , on both cyber-dependent and cyber-enabled crimes. The phenomenon has been faced in detail, starting from its borderless nature to its dangerousness. This Model supplies a discipline on criminalization and investigation of cybercrime, taking inspiration from the Budapest Convention, with the support of experts from Commonwealth countries.

It is articulated in three parts: the first section defines the phenomenon and related concepts; the second one analyzes substantive criminal laws, indicating

[67] Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS, August 2011, Abuja
[68] SADC Model Law on Computer Crime and Cybercrime, 2013
[69] African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014, Malabo
[70] The Commonwealth, Office of Civil and Criminal Justice Reform Model Law on Computer and Computer related crime, 2017

prosecutable offences; the third part provides for procedural laws, guarantees and law enforcement mechanisms.

According to a conceptual point of view, the Budapest Convention, as the other regional legislations mentioned before, made a worldwide impact against cybercrime. But, that was not enough; therefore, the two United Nations Conventions, UNTOC [71] (United Nations Convention against Transnational Organized Crime) and UNCAC[72] (United Nations Convention against Corruption), have conducted a "supplementary" and integrative role, mostly in reference to the establishment of collaborative and cooperative relations, at international level.

The United Nations Convention on Transnational Organized Crime, also known as Palermo Convention, drafted in 2000, is the main legal instrument against all types of criminality, because it contains innovative laws about investigations, electronic surveillance and cooperation. Based on this Palermo Convention, there was and still is the Giovanni Falcone's anticipatory and progressive vision, who, just a month before the Capaci Bombing, participated to the First Session of the UN Commission on Crime Prevention and Criminal Justice: in spite of the different ideas expressed in this occasion, international judicial cooperation was considered the necessary solution to face the transnational dimension achieved by a multitude of criminal phenomena. One of the most remarkable characteristics of UNTOC is its flexibility and scope, which allowed to also include new manifestations of criminality, like cybercrime.

In reference to the latter, UNTOC finds its most incisiveness in the cyber-organized crime phenomenon, which as it was said, corresponds to cyber offences perpetrated by an associated group of people.

Palermo Convention is articulated in a central part and three additional protocols. In the core section it is possible to distinguish general provisions, substantive provisions and criminalization, procedural provisions, law enforcement and international cooperation. The additional protocols are focused on specific matters: the first one analyzes prevention, suppression and punishment of trafficking in persons, especially women and children; the second one is against smuggling of

[71] United Nations Convention against Transnational Organized Crime, Palermo, 2000
[72] United Nations Convention against Corruption, Merida, 2003

migrants, by land, sea and air; the third one concerns Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. Among all the articles of the Convention, article 28 has a prevalent role, since it contains three recommendations to Member States: first of all conferring importance to consultations with scientific and academic communities, in order to collect information and strategies about organized crime in the world; moreover, this article underlines the relevance to develop and elaborate definitions, standards and common methods; and at last, it highlights the possibility to each State to monitor and assess policies and practical measures. It can be said that this article may originate a remarkable innovation process in the fight against cybercrime, in full compliance of the fundamental rights and freedoms.

As every international treaty, UNTOC necessitates of specific control mechanisms and constant supervision, to verify its correct implementation; for this reason, the Review Mechanism[73] was established by the Conference of the Parties in 2018. It allowed to overcome obstacles which impeded the full application of UNTOC, and to develop an incisive response against global criminal phenomena, through repressive and preventive activities, together with investigative techniques. Therefore, it would be possible to promote a harmonization of legislations to combat organized crime, both through incriminatory laws and the improvement of mechanisms of judicial cooperation among States: starting from sharing information for a more functional collaboration, identifying blanks which make this phenomenon difficult to prosecute, to further legislative reforms.

In 2020, on the Tenth Conference of the Parties and of the Twentieth Anniversary of the Palermo Convention, the "Falcone Resolution"[74] was approved unanimously. Taking inspiration from the Italian magistrate's ideas, it encourages the establishment of new investigative instruments, in light of the technological progress, with the support not only of experts, but also of judicial police and judges. The Falcone Resolution may be applied to all organized crime associations, both

[73] UN Resolution 9/1: Establishment of the Mechanism for the Review of the implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto

[74] UN Resolution 10/4: Celebrating the twentieth anniversary of the adoption of the United Nations Convention against Transnational Organized Crime and promoting its effective implementation

historical and modern ones, like cybercrime: this means restating again the flexibility nature of UNTOC, which can be applied also to more dynamic and evolved forms of criminal activities[75].

The United Nations Convention against Corruption, or Merida Convention, is the universal anti-corruption instrument, created in 2003; corruption is a crime perpetrated in every part of the world, reason why it is necessary to eradicate it with an international and global action, which is a United Nations Convention.

UNCAC has a far-researching approach, in order to create a unique instrument to develop a uniform response against a worldwide problem. It is articulated according to the same specific method used for UNTOC: general provisions, preventive measures, criminalization and law enforcement, international cooperation, asset recovery, technical assistance and information exchange. Certainly, the section to be taken in consideration as a model, applicable also to other types of offences, is the one on international cooperation among Member States, and with international organizations, providing also mutual legal assistance in investigations and prosecutions.

The United Nations Conventions on Transnational Organized Crime and Corruption are the two main examples that encourage improvement and incite Member States to take stable relations, for the purpose of international collaboration and cooperation, to counter crimes expanding worldwide and like wildfire. Besides them, the United Nations enjoys also of other technical instruments: in 2007, a specific section created by the UN General Assembly, the United Nations Office on Drugs and Crime (UNODC) formulated the so-called "Model Law on Mutual Assistance in Criminal Matters"[76], a document entirely based on mutual assistance among countries in criminal matters. In this soft-law regulation, the importance of the principle of mutual assistance is stated, providing for general provisions and disciplines that suggest international collaboration in order to prevent and combat crime. Recalling principles of sovereignty, reciprocity and confidentiality, the mutual assistance is brought about through specific instruments such as extradition,

[75] A. BALSAMO, *Il contrasto internazionale alla dimensione economica della criminalità organizzata: dall'impegno di Gaetano Costa alla "Risoluzione Falcone" delle Nazioni Unite*, Sistema Penale, 2020

[76] UNODC, *Model Law on Mutual Assistance in Criminal Matters*, Vienna, 2007

confiscation, exchange of information and experience. A specific section of this Model Law concerns assistance in relation to computers, computer systems and computer data, aiming for a reciprocal support among States in the digital dimension. In addition to this legal document, in 2009, UNODC elaborated the "Current Practices in Electronic Surveillance in the investigation of serious and organized crime"[77], with the aim to enhance global practices against crime with the use of electronic surveillance, training law enforcement to apply them for investigations of serious crime. This document consists of a guide to assist legislators, police, experts to the implementation of these practices, balancing them with the individuals' right to privacy.

Thanks to the General Assembly Resolution 65/230 [78], together with the Commission on Crime Prevention and Criminal Justice Resolutions 22/7[79] and 22/8[80], the Global Programme on Cybercrime was established, with the aim to assist Member States in the fight against information technology attacks, through capacity building and technical assistance. Particularly, the importance of international cooperation was underlined, establishing an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. The Global Programme wants to improve the efficiency and efficacy of investigation and prosecution, preserving human rights; it supports coordination with domestic instruments and it strengthens communications among Member States and governments.

Both the Global Programme and the intergovernmental expert group were established in 2011, under the constant assistance of the UNODC, which produced also, on the advice of USA, UK, Australia, Japan and others, a very useful portal: SHERLOC, or Sharing Electronic Resources and Laws on Crime Portal. It is an instrument created in order to facilitate the spread of information, referring the

[77] UNODC, *Current Practices in Electronic Surveillance in the investigation of serious and organized crime*, Vienna, 2009

[78] UN General Assembly Resolution 65/230: Twelfth United Nations Congress on Crime Prevention and Criminal Justice

[79] UN General Assembly Resolution 22/7: Strengthening international cooperation to combat cybercrime

[80] UN General Assembly Resolution 22/8: Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime

implementation of Transnational Organized Crime Convention and its Protocols. Despite this specific aim, SHERLOC Portal has been used also for other types of offenses, like corruption, cybercrime, money laundering etc. It analyzes specialized procedures and disciplines to facilitate investigation and the application of practical measures such as extradition, letters rogatory and mutual assistance.

As information technology platform for all intents and purposes, SHERLOC is composed of a lot of databases: the case law database, containing jurisprudence, where users are allowed to be aware on modalities used by Member States' courts to judge criminals; legislation database, an electronic storage of domestic and conventional legislations; bibliographic database; CNA directory, section that receive and answer extradition and letters rogatory requests; and at last, the contributor access, a technical mean, dedicated to the platform team, in order to update it constantly[81].

In addition to this platform, UNODC put efforts in the "Artificial Intelligence for the safeguard of children" initiative, efficient all over the world, to educate artificial intelligences to combat sexual abuses on minors, and related materials.

Despite disciplines deriving from different regional organizations, a common element of all of them is to strengthen international cooperation and collaboration, seen as the one and only solution to combat cybercrime.

Recently, "the 2019-2021 Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) was established by the General Assembly in its resolution 73/27[82]. The OEWG's mandate was to develop further rules, norms and principles of responsible state behavior, study the possibility of establishing a regular institutional dialogue under auspices of the United Nations, continue to study existing and potential threats in the sphere of information security, how international law applies to the use of ICTs by states, as well as confidence-building and capacity-building measures in this field, and to submit reports on the results to the General Assembly. The 2019-2021 Group of Governmental Experts on advancing responsible state

[81] UNODC, *SHERLOC Sharing Electronic Resources and Law on Crime*

[82] UN General Assembly Resolution 73/27: Developments in the field of information and telecommunications in the context of international security

behavior in cyberspace in the context of international security (GGE), on the other hand, was established by the General Assembly in its resolution 73/266[83]. Similarly to the OEWG, the GGE's mandate was to continue to study measures to address existing and potential threats in the information security sphere, norms, rules and principles of responsible state behavior, confidence-building and capacity-building measures, as well as how international law applies to the use of ICTs by States, and to submit a report of the result to the General Assembly. While the OEWG report was more general in scope, describing overall issues in the context of new technology and international security, the GGE focused on the implementation of the already existing voluntary non-binding norms of responsible state behavior. The 2021 GGE and OEWG reports are important non-binding intergovernmental reports on the impact of new technology on international security.

In April 2021, the Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime agreed on recommendations ('IEG Recommendations' or 'Recommendations') on how best to address issues of cybercrime through the implementation of legislation and frameworks on effective criminalization, law enforcement and investigation, electronic evidence and criminal justice, international cooperation, and prevention. The Recommendations emphasize the importance of the need for consistent terminology. In general, States are asked to strengthen existing networks, for exchanging information, best practices and evidence, and also to rely on INTERPOL channels, and make use of such networks before formally requesting mutual legal assistance. The Recommendations, at various places, emphasize the importance of effective international cooperation. They stress the importance of having national laws in place which authorize or enable States to cooperate internationally. They further emphasize the importance of international cooperation with respect to the sharing of electronic evidence. Moreover, they support the establishment of rapid response mechanisms and direct channels of communication through liaison officers. Also, States are encouraged to establish joint investigative teams. The Recommendations further suggest that national laws should be put in place which ensure the real-time collection of traffic

[83] UN General Assembly Resolution 73/266: Advancing responsible State behaviour in cyberspace in the context of international security

data and content. The Recommendations also suggest that States should consider enacting legislation that ensures the collection, preservation, authentication and admissibility of electronic evidence. Furthermore, it is recommended that States consider establishing traffic data, content data, subscriber data, and other "digital" data used for the commission of a crime as electronic evidence in their domestic laws. A range of the recommendations also stress the importance of capacity-building measures. Moreover, many provisions stress the importance of strengthening the capacity of practitioners, in particular law enforcement officers, to deal with issues of cybercrime. The recommendations further suggest training, networking and joint meetings for law enforcement officers, central authorities and lawyers to adjudicate cases. It was also emphasized that especially developing countries may need more support for capacity- building than other countries"[84].

1.5 The necessity of a United Nations International Convention on Cybercrime

The international framework on cybercrime is quite wide. Indeed, in the last years, a lot of states has focused so much on the "digital sovereignty", drafting many legislations, both with regional and international natures, to counter this phenomenon as much as possible. Nevertheless, cybercrime has not been eradicated in a very efficient way. Information technology attacks are multiples, which damage populations across-the-board: attacks on infrastructures, governments and digital platforms.

For this reason, the necessity of a uniform and harmonized convention is born, operating at international level, to supply for the little incisiveness of regional legislations previously mentioned, so establishing a global common system of rules. Despite the Budapest Convention constituting a remarkable step forward, since it is the very first regulation on cybercrime, it presents a lot of blanks: first of all, this convention disciplines the criminal phenomenon only for a restricted circle of

[84] "Overview of existing instruments, recommendations and other documents on countering the use of information and communications technologies for criminal purposes" elaborated by the Chair of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

States of the world, some Council of Europe Member States and foreign ones; it does not respond to the necessities and needs of world's countries, but only to some of them, the signatory ones. Furthermore, this legislation is focused on specific types of offences, basically cyber-dependent crimes; even it has been actualized recently through its Second Additional Protocol, the Budapest Convention is limited to harmonize domestic penal systems and related dispositions on cybercrime. In addition, an efficient and effective discipline on electronic evidence is insufficient: actually, it is essential if a concrete collaboration among States is reached, because it would allow a favorable exchange of information and elements, usable during criminal proceedings. With a specific discipline, electronic evidence could be saved and stored all over the world, since it has a borderless nature because produced into cyberspace, facilitating a widespread use of them, without territorial limits. Even though this Additional Protocol introduces improving mechanisms, there are still lacunae, especially regarding conditions of use.

The other regional conventions and models formulated, like the African Union Convention or the Commonwealth Model Law and others already mentioned, are restricted: besides the emulation of the Budapest Convention, they added single needs, deriving from each states' problems, counting on a narrow-type cooperation and collaboration.

As it was said many times in this dissertation, cybercrime is a wide-range phenomenon, which involves the whole world: an equally broad response is needed to face this borderless crime, which may hit through a uniform action, independently from the geographical location. Such a broad work is conducted by the United Nations.

Since its birth, UN has spread and established roots inevitably in the world, having competences on a lot of fields. Collaboration, cooperation and solidarity are the base of this efficient international organization.

As it was said, in order to achieve its purposes, the United Nations, more specifically its General Assembly, established some specialized entities on designed scopes: OHCHR, the Office of the High Commissioner for Human Rights; UNDP, United Nations Development Programme; UNHCR, United Nations High

Commissioner for Refugees; UNICEF, United Nations International Children's Emergency Fund, etc.

Among these entities and agencies, the United Nations International Computing Centre (UNICC) is the leading provider of digital business solutions within the UN system. UNICC is committed to deliver reliable digital solutions driven by best practices. With its world-class technology and state-of-the-art infrastructure, UNICC is ready to offer shared solutions to United Nations organizations and other international organizations with similar missions and values. As a section belonging to the United Nations, UNICC has also the aim to reach and fulfill the 2030 Agenda for sustainable development, with the 17 Sustainable Development Goals, or SDGs, for achieving peace and prosperity for people and the planet. These goals are common objectives which involve every State and individuals: nobody is excluded and no one is to be left behind.

In particular, the main goal to reach for UNICC is the 16th one, about peace, justice and strong institutions, also through the use of technology: the latter has enormous potential to achieve the SDGs with for instance blockchain, automation, Artificial Intelligence and Big Data.

About the cybercrime issue, UNICC is active, indeed in today's digitalized world, cybersecurity has emerged as a matter of importance for international organizations. The potential consequences of a weak cybersecurity posture go beyond the disruption of ICT infrastructure and systems. For this reason, UNICC's information security services cover cyber security oversight and governance as well as a whole spectrum of operational components; it also offers data and analytics services across the entire business digital spectrum, and provides computing infrastructure resources that to easily manage networking, data centers and infrastructure elements for their business needs and application stack[85].

Besides UNICC, which is focused mainly in the technological field, also the United Nations Office on Drugs and Crime (UNODC) has a remarkable importance. Indeed, it was founded with the aim to assist UN to address a global coordinated response to trafficking in drugs, prevention of crime and specific serious offences like terrorism, organized crime and so on. Results made by UNODC, thus by UN,

[85] See www.unicc.org

are UNTOC and UNCAC Conventions, already mentioned, respectively on organized crime and corruption. Therefore, the United Nations is successful for contrasting a lot of criminal phenomena, counting on the joint action of the Member States. Among all different operations that UN may made, they also formulate conventions and legislations which address to Member States' needs, elaborated after long discussions, and analyzing even meticulous aspects. Once the proposals are presented, based on each nations' circumstances, Member States discuss actively on which solutions may be the best to take, balancing restrictive measures to fundamental rights and freedoms.

Also, on cybercrime, countries of the world have a common voice to ask for a uniform and international convention, which may discipline this phenomenon, starting from definitions, to more sophisticated mechanism to counter it. Conventions drafted by regional organizations have mitigated the effects and consequences of the crime, but they do not have a strong incisiveness to eradicate it at all: it is not possible to combat a transnational crime without a transnational-type instrument. Despite UNTOC focusing more on organized crime, it refers also to other kind of crime, through its innovative laws on cooperation. As regard cybercrime, it compensates for the Budapest Convention restricted dimension, but it is not enough even so. Therefore, a new international legal instrument is necessary to counter cybercrime, pursuing global harmonization and a collective incrimination, and balancing interests of all Member States. The more appropriate models to follow for the elaboration of a new UN convention, through the UNODC support, would be UNTOC and UNCAC, providing for a similar structure with general provisions on definitions, scope and fundamental principles, substantive provisions and criminalization with a detailed analysis of cyber-dependent and cyber-enabled crimes, procedural provisions and practical measures for juridical cooperation, law enforcement, international cooperation, together with capacity building and technical assistance, especially to those developing countries.

The proposal of a new United Nations Convention on cybercrime was presented many times over the years. The impulse arose from the will of some States, including the Russian Federation, China and developing others, to negotiate a new international legal document, effective worldwide.

Indeed, these countries did not participate to the elaboration of the Budapest Convention, and for this reason they deemed to express their needs and requirements necessary, in the light of the constant evolution of criminal offenses.
Formerly, in 2010, the Russian Federation proposed a treaty on cybercrime to the 12th UN Crime Congress, but the negotiation failed because of discordance on sovereignty of States and human rights protection. Nevertheless, Commission on Crime Prevention and Criminal Justice (CCPCJ) established, after a request by the General Assembly, an open-ended intergovernmental expert group (EGM), to conduct a comprehensive study on the criminal phenomenon. EGM and UNODC's Global Programme have dealt with cybercrime in detail, analyzing aspects and theorizing solutions to counter it.
If on the one hand there were countries which pushed to obtain an international convention on cybercrime for years, on the other hand Western countries, like European Union Member States or the United States of America, originally were reluctant to the formulation of a new document. They considered the Budapest Convention a suitable instrument to combat the crime, with the need to be periodically actualized in relation to new technologies and criminal offences, as it was made partially with the Second Additional Protocol.
Only subsequently, due to the strong dangerousness and diffusion of cybercrime, the necessity of a new United Nations convention has been recognized at global level, in order to address the crime with the same incisiveness and efficacy provided for UNTOC and UNCAC.
Through the 2019 Resolution 74/247[86], the United Nations General Assembly established an "*Ad Hoc* Committee to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes". Not by chance, this committee deals with the use of ICTs, in order to consider both cyber-dependent crimes and cyber-enabled crimes, which misuse these instruments to commit criminal offences. The will to formulate a focused solution to combat this phenomenon is the driving force that pushes and encourages Member States to collaborate among each other, for a common purpose.

[86] UN General Assembly Resolution 74/247: Countering the use of information and communications technologies for criminal purposes

CHAPTER 2

THE ELABORATION OF A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

SUMMARY: 2.1 The *Ad Hoc* Committee – 2.2 The First Session of the *Ad Hoc* Committee – 2.3 The First Intersessional Consultation of the *Ad Hoc* Committee dedicated to multi-stakeholders – 2.4 The Second Session of the *Ad Hoc* Committee – 2.5 The Second Intersessional Consultation of the *Ad Hoc* Committee dedicated to multi-stakeholders – 2.6 Contextual Developments to the new Convention on cybercrime

2.1 THE *AD HOC* COMMITTEE

Article 13 of the Charter of the United Nations mandates the General Assembly "to initiate studies and make recommendations for the purpose of promoting international cooperation in the political field and encouraging the progressive development of international law and its codifications […]"[87]. In order to fulfill this task, the General Assembly has established *Ad Hoc* Committees for the purpose of developing legislations on international law on specific topics. Generally, legislative bodies and organizations use this method to counter specific issues, both political or social ones. Indeed, these committees are established to analyze phenomena in detail and formulate new solutions, also promoting the creation of relations and cooperation among States[88].

The United Nations General Assembly had noticed, after an accurate analysis of the evolution of technologies, that ICTs have had a great and galloping development, so creating new opportunities for perpetrators to commit crime, rising also the level of criminality in the world. The potential risk of the misuse of emerging IT systems and instruments, like artificial intelligence, brought the

[87] Art.13 of the Charter of the United Nations
[88] See www.legal.un.org

General Assembly to stress and enhance coordination and cooperation among States, to improve national legislations and capacity building of authorities.

Despite the existent expert groups on cybercrime being useful to study and learn the phenomenon, it cannot be considered enough to prevent and combat this crime, as also the other methods created by the United Nations Office on Drugs and Crime (UNODC) such as the Global Programme and the SHERLOC protocol. They allowed to facilitate exchange of information, experience, technical assistance, but without providing for incisive and focused actions to eradicate or at least regress cyber offences. Until 2019, the United Nations supplied studies, mechanisms of sharing, non-binding legislations, or some disciplines taken from UNTOC. Therefore, the General Assembly, through its resolution 74/247, established the *Ad Hoc* Committee on cybercrime, providing for an open-ended intergovernmental group of experts, representatives of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

It is not the first time that the General Assembly has created an *Ad Hoc* Committee relied on UNODC to counter widespread crimes; in fact, this method was used for the elaboration of UNTOC and UNCAC, to combat organized crime and corruption respectively.

The purpose of these committees is to draft a convention that may be significant for each Member State, allowing delegates and representatives to express their opinions and purposes on the work, and the aspects that should be analyzed in detail.

The base on which these committees are founded is the dialogue among parties, in order to discuss about their necessities, finding solutions that could be optimal for everyone. Therefore, in this specific case, the intention of the body is to take into account UNTOC and UNCAC, especially in reference to their structural models, along with the national and regional efforts made, with the objective to continue a path already started.

The composition of the "*Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for criminal purposes" is peculiar: in fact, it is

chaired by Algeria, supported by thirteen vice-chairs from Egypt, Nigeria, China, Japan, Estonia, Poland, Russian Federation, Dominican Republic, Nicaragua, Suriname, Australia, Portugal and USA[89]. Together with the technical team, there are delegates from Member States, the Observers, and the so-called multi-stakeholders who are: representatives of global and regional intergovernmental organizations, including representatives of UN bodies, specialized agencies and funds, as well as representatives of functional commissions of the Economic and Social Council; representatives of non-governmental organizations that are in consultative status with the Economic and Social Council, in accordance with the Council; representatives of other relevant non-governmental organizations, civil society organizations, academic institutions and private sector[90].

The role of the aforementioned stakeholders is essential because they may suggest interesting points of view and causes for reflection, which could help for the formulation of practical measures to counter cybercrime: many people belonging to these organizations are effectively subjected to information technology attacks, they suffer a real damage of their human rights.

Some stakeholders are entities, for instance INTERPOL, that may offer great suggestions, especially on law enforcement and investigative operations. Others are expert bodies which may provide detailed analysis of the phenomenon, its various manifestations and characteristics, in order to combat it purposely. In addition, the *Ad Hoc* Committee is composed also of members from the so-called private sector, corporations, which make their own knowledge and devices available, in order to make understand how to use information and communications technologies, for countering cybercrime, with a positive intention.

As it was said, offences in the digital environment have a significative impact on people's lives. For this reason, giving full consideration to the respect for states' sovereignty and the protection of human rights and fundamental freedoms, the *Ad Hoc* Committee has the task of elaborating a comprehensive Convention with the objectives of promoting and strengthening measures to prevent and combat the use of ICTs for criminal purposes, while protecting users from such crimes. More

[89] See https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[90] See A/AC.291/INF/3/Rev.1 Document on the List of Participant published in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

specifically, in accordance with the proposal on scope and purposes elaborated by the Chair of the aforementioned Committee, the Convention should provide also practical tools to enhance technical assistance among State Parties and build the capacity of national authorities, especially for the benefit of developing countries, and reinforce measures to promote the exchange of information, experience and good practices. Finally, the Convention has to promote, facilitate and support international cooperation, as the main solution to counter this criminal phenomenon[91]. The aim of the *Ad Hoc* Committee, besides pursuing the objectives just mentioned, is to lead a careful and accurate work: the negotiation of a global treaty may on the one hand reinforce some approaches to cybercrime, but on the other hand it may sacrifice some rights and freedoms (for instance the freedom of expression is frequently targeted).

The *Ad Hoc* Committee follows a precise scheme for the organization of its work, indicated also in the "Roadmap and mode of work of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" proposed by the Chair and the UNODC Secretariat. Sessions are held in New York and Vienna, together with the so-called intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention, in accordance with paragraph 10 of the General Assembly resolution 75/282.

By taking into account the experience of past *ad hoc* committees to elaborate UNTOC and UNCAC, and the interrelation among articles and logic flow in the text of a convention, the formulation of this new legislative document should be based on discussions about proposals and contributions made by Member States and the Chair: each session deals with a specific topic, and delegates debate, trying to find a common ground[92]. At the end, the entire Committee adopts and approves the draft reports made by the UNODC rapporteur.

---

[91] "Proposals on objectives and scope of the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" elaborated by the Chair of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

[92] "Proposed roadmap and mode of work of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" elaborated by the Chair of the *Ad Hoc* Committee

2.1 THE FIRST SESSION OF THE *AD HOC* COMMITTEE

The United Nations General Assembly, in accordance with the highest roles of the *Ad Hoc* Committee, more specifically the Chair and UNODC Secretariat, scheduled the First Session for the Elaboration of a new convention through the decision 76/552[93], from 28th February to 11th March 2022, after a lot of postponement because of the Covid-19 pandemic.

During the weeks before the session, many States presented some proposals regarding formation, structure and content of the future convention. Among them, certainly the Russian proposition is worthy of particular attention, not only because it was presented firstly, but above all because the Russian Federation is the country which has pressed more for the elaboration of an international legal document on cybercrime.

The Russian Federation's proposal corresponds to a real draft of a convention, where universal disciplines and implementational measures are analyzed in detail: it is articulated in seven chapters, preceded by a preamble on which typical principles of international law are stated, along with fundamental rights and freedoms of individuals. All disciplines of the future convention, and in this case of its Russian Federation's draft, should fit together with domestic law principles, and in compliance with it. Moreover, within the preamble, the importance of cooperation and collaboration among States is disclosed, in order to enhance the incisiveness of means and practical instruments, providing for a detailed legislative prevision, not harmful for essential values.

The first chapter of the Russian proposition concerns mainly general provisions, objectives and purposes that the convention should reach, such as to strengthen means and create preventive measures to ward off damage, improving also the efficiency of international collaboration. The principle of sovereignty of countries is restated many times in the draft, as the pivot of the whole Russian discipline, to preserve as much as possible domestic principles and rights. Peculiarity of this chapter is the attention reserved to fundamental notions connected to cyberspace

[93] UN General Assembly Decision 76/552: *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for criminal purposes

and cybercrime, so avoiding problems on the reception of concept in national legal systems, and providing also for definitions valid at international level. Among them, “property” notion is surely remarkable because it comprehends not only material things, movable and immovable, but also what is intangible, like money in banks, digital financial assets, digital currency, cryptocurrency and legal documents.

The second chapter is dedicated to substantial and procedural aspects of cybercrime, focusing on criminalization, criminal proceeding and law enforcement. It is partitioned in two sections: the former analyzes the substantial point of view, so all criminal offences belonging to the cybercrime category, such as unauthorized access, spread of malwares, sexual exploitation of children through the Internet; the latter concerns the procedural side, criminal procedures, law implementation and enforcement in countries.

The following chapter deals with measures to prevent and combat offences and other unlawful acts in cyberspace, including a set of conducts which States may develop in order to enhance domestic mechanisms, innovating them to combat this type of crime.

The fourth chapter, as the second one, is divided in two sections: the first one is focused on general principles of international cooperation, more specifically reciprocity and mutual assistance ones and the support given by INTERPOL, regulating the recourse to some practical instruments like extradition. An innovative element included in this chapter is the use of electronic devices to conduct questioning or other procedural activities through video or telephone systems. The second section concerns patrimonial measures like seizure and confiscation, even in case of intangible elements, but existing in cyberspace, as IT documents or registrations etc.

The fifth chapter underlines Member States of the convention are held to provide instruments and means specialized to technical assistance and ICTs training (develop, implement, improve specific training programs for combating ICTs crimes in domestic and international legal systems). Countries are encouraged to collaborate among each other, assisting developing ones for the purposes of capacity building and updates of techniques.

The sixth chapter analyzes the convention's mechanisms of implementation, determining useful means to actualize and promote international collaboration. In this chapter, activities, procedures and working methods are studied in detail, in order to reach the convention's purposes. For achieving these objectives, the Russian Federation suggests to establish an international technical commission, to assist countries and verify the correct implementation of the convention.

And the last and seventh chapter lists final dispositions of the convention, in which are indicated the modalities for the enforcement and compliance of it with domestic rules. In case of contrast among countries, the litigation may be solved through the classic methods foreseen by international law, such as negotiation, conciliation or arbitration. The ultimate discipline of the aforementioned chapter is dedicated to the modalities of signature, ratification, acceptation, approval and entry into force of the convention, in conformity with the procedures defined by the *Ad Hoc* Committee and international law[94].

Besides the Russian Federation, which stood out for its proposal compared to the others, since it is a real draft of a convention, also other States elaborated some solutions to suggest the *Ad Hoc* Committee, including the United States of America. In their proposition, the importance of an open-ended, comprehensive and transparent formation process of a convention was stressed a lot, to allow a spread knowledge of manifestations and forms of cybercrime. The indicated disciplines strive for the adoption of practical instruments by single Member States to provide for the actualization of domestic legal systems, along with international cooperation and collaboration mechanisms. In this proposal it was restated to avoid the potential duplication of regulations already established in the Budapest Convention and in the Palermo Convention, opting for the introduction of brand-new and innovative elements to counter this phenomenon constantly evolving. The mandate of the *Ad Hoc* Committee should be focused on the development of instruments which encourage a response at international level that may define and sanction criminal conducts perpetrated within cyberspace. The use by populations of networks, computer systems, software facilitate more the possibility to steal this information

[94] See the Russian Submission related to the first session of the *Ad Hoc* Committee in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

and then reuse it; the purpose is trying to track and identify the authors of these behaviors, even if they are covered by anonymity.

A discipline that should be included necessarily in the future convention is about electronic evidence, especially for exchanging of information and experience among countries of the world.

Cybercrime activity is global, reason why it is necessary that all Member States adopt harmonized and common legislation, which criminalize every manifestation of this phenomenon, protecting also human rights and fundamental freedoms. Aware that future is uncertain, because computers, social networks and systems change, the United States' proposal aims to regulate authors' illicit conducts, not single instruments, in order to cover as many cases as possible.

The core of this proposition is articulated in two points: actualization of domestic legislations, and effective international collaboration as well as cooperation which may guarantee legal and technical assistance: to avoid the disproportion among developed countries and developing ones, to create mechanisms to provide for financial contributions and support capacity building. The importance of the active participation of individuals and groups belonging to non-governmental organization, civil society, or private sector may enhance and improve the awareness that threats related to cybercrime affect common people mainly[95].

The Australian proposal has the aim to find the best path to combat cybercrime. The answer to this type of offence may be found in international collaboration and cooperation, together with proper preventive measures. The new convention has to take inspiration certainly from the UN Conventions against Transnational Organized Crime and Corruption, as well as the Budapest Convention, which moved up such an actual theme. With regard to structure and purposes, Australia's proposition wants to elaborate a new international legal document which could offer the opportunity to create a system of harmonized and common rules of law, concerning mostly specific criminal conducts. Indeed, it is necessary to criminalize not only offences ascribable to the original concept of cybercrime, thus linked to software, malwares, personal information in computers, but also to those cyber-

[95] See the USA Submission related to the first session of the *Ad Hoc* Committee in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

enabled crimes such as trafficking in drugs, human beings and offences against individuals (instigation to suicide, sexual exploitation and abuse of minors)[96].

Even the European Union, through its role of observer at the United Nations, presented a contribution to the *Ad Hoc* Committee. In detail, EU and its Member States underline that the future convention against the use of ICTs for criminal purposes should be considered aa a practical instrument for law enforcement and implementation of disciplines sanctioning cybercrime. As it was said also in the other propositions, the main aim is international collaboration and cooperation among States. Indeed, the EU encourages the creation of substantial laws criminalizing all types of crimes in the cyber-dimension, both cyber-dependent and cyber-enabled ones, with clear and precise definitions, following the principle of legality, fair and equal trial, privacy. Regardless of whether these crimes are conducted online or offline, the protection of human rights has to be full and constant, balanced to an incisive legislative provision, which may counter cybercrime actively.

Moreover, the European Union exhorts countries to improve specific mechanisms of collaboration, especially about investigation, capacity building, exchange and sharing of evidence and experience, obviously with respect to the principle of sovereignty[97].

These proposals just explained were presented to the UNODC Secretariat, in view of the first session of the *Ad Hoc* Committee. They are very generic drafts, which may constitute suggestions on themes to face during the future meetings.

The First Session of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes was held in New York, from 28th February to 11th March 2022, and was attended by 140 Member States of the world, which participated actively.

[96] See the Australian Submission related to the first session of the *Ad Hoc* Committee in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[97] See the European Submission related to the first session of the *Ad Hoc* Committee in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

More specifically, during these meetings, the *Ad Hoc* Committee dealt with a lot of topics regarding the formulation of a new convention, following the planning provided according to the "Provisional Agenda".

The importance and urgency of this convention was restated, especially pursuant the Covid-19 pandemic, which caused a strong increase of cybercrime, through hacker assaults, mostly to infrastructures such as hospitals.

This first session of the *Ad Hoc* Committee was organizational and generic mainly, indeed during its ten meetings, it handled with discussions on how to frame objectives, scope, structures and future working methods.

Essential topics, analyzed many times by the States, both during the general debate and discussions about purposes and structure of the future conventions, are: the necessity of a full protection of human rights, fundamental freedoms, right to privacy and safeguard of personal data; capacity building operations and technical assistance, especially to those developing countries; international cooperation and collaboration, in order to conduct joint and coordinated actions for prevention, investigation and prosecution.

All discussions followed the guidelines indicated by the Chair's proposals, H.E. Ms. Faouzia Boumaiza Mebarki; Member States and Observers, together with the so-called stakeholders, shared their opinions in relation to these propositions, bringing some changes, and focusing on noteworthy themes.

The most debated Chair's proposal was certainly the one on objectives, purposes and scope of the convention: indeed, it underlined the importance to promote and strengthen measures to prevent, combat and in general counter the use of information and communications technologies for criminal purposes, facilitating the collaboration among States of the world, especially with practical instruments which may enhance technical assistance and reinforce capacities to combat cybercrime.

Within the proposal, some points were indicated explicitly, which would belong to the content of the convention, such as definitions of offences and legal institute, types of crimes, but mostly the prevision of substantial and procedural laws: the former in order to criminalize those conducts brought about, thus establishing the criminal liability of authors; the latter to intervene through practical means, joint

operations to facilitate investigations and proceedings. The exchange of information and experience may be essential, not only because they could be considered element of proof, but also because they could constitute a great step forward to dissolve cybercrime.

Another proposal formulated by the Chair which stimulated interest among Member States is on the structure of the convention. It was approved without particular amendments by delegates, and it is divided in nine sections, that analyze various aspects of the crime: the preamble brings the content of the convention forward and specify the objectives; general provision, mainly on definitions of legal institutes; criminalization, through substantial laws; procedural measures and law enforcement; international cooperation; technical assistance, with sharing of information and experience; preventive measures; implementation and application of the convention; final dispositions.

During these debates, Member States restated many times to strengthen as much as possible domestic defenses and institutions, in order to prevent cybercrime. A lot of developing countries showed their will to participate actively to the elaboration of the convention: thus, several needs emerged from the countries of the world, supporting for a clear and inclusive process of formation of the new legal document, avoiding the possibility for stronger countries to override developing ones.

Common belief was to take inspiration from previous conventions: the United Nations Convention against Transnational Organized Crime, also known as UNTOC or Palermo Convention, and the United Nations Convention against Corruption, the so-called UNCAC or Merida Convention. Besides them, there is also the Council of Europe Convention against cybercrime, or Budapest Convention.

These historical antecedents are crucial because they provide foundations on which the actual United Nations Convention on cybercrime may be built, and becoming also models to follow about structure, objectives and glossary, as a narrative thread. The new convention, as it was said by various Member States, does not become a copy or a simple regulation, just more actualized than those previous ones. It has to be inspirational for creating new law, which may facilitate cooperation and collaboration among countries, promoting joint and coordinated operations against

cybercrime, and in general every manifestation of criminal activity through the use of information and communications technologies.

Some common themes in Member States dissertations are about the inclusion in the future convention of a specific section dedicated to the definition of the cybercrime phenomenon, together with its forms (cyber-dependent and cyber-enabled), and creating substantial and procedural laws.

More specifically, a strategy mentioned during the meetings is to apply these laws, in respect to principles of legality, proportionality and sovereignty of States.

The latter was a very debated problem, in order to avoid that powerful countries would override developing ones, monopolizing them, instead of conduct joint actions.

Because of the rapid evolution of cybercrime, a lot of Member States suggested to provide for definitions, valid not only for actual conducts, but also for future ones, after the eventual technological progresses and changes.

During this first session, many representatives of stakeholders had the floor, for instance INTERPOL, which underlined the fundamental role that police has, both at national and international level, for the defense of victims; indeed, law enforcement act immediately, at the time that the damage is perceived and reported, trying to identify perpetrators.

One of the main differences of ideal among Member States was on the modalities of treatment and inclusion of international human rights within the future convention.

Many Western countries and Non-Governmental Organizations expressed their will to deal with this topic in a very detailed and accurate way, in order to avoid some mechanisms and instruments may interfere with fundamental rights and freedoms.

Other countries, such as the Russian Federation, China, Iran, deemed that an excessive emphasis on human rights may weaken all means to fight cybercrime, so preferring the focus on legal institute and disciplines.

All these concepts were reaffirmed during the exchange of preliminary opinions on the key elements of the convention.

Cybercrime is a threat with a transnational dimension, which has to be faced by the States of the world, just for the transversal nature of cyberspace. The latter has not

geographical borders, reason why everyone may become a potential victim. The objective that Member States has to reach is to combat cybercrime with incisive instruments and methods, for the protection of fundamental rights and freedoms. To quote the Jordan's delegate: "No country is immune to cybercrime: everyone belongs to cyberspace".

Despite different opinions and indications expressed by each Member State, the First Session of the *Ad Hoc* Committee had a great success, reaching common and general leanings about the importance to define the phenomenon and its manifestation, promoting international cooperation and collaboration for capacity building and technical assistance, involving experts from civil society, Non-Governmental Organizations, universities in, for studying the modalities to counter cybercrime.

Thus closes the First Session of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, with the adoption of all draft reports about the general debate, objectives and purposes, structure and discussion on the future working methods of the *Ad Hoc* Committee.

2.3 THE FIRST INTERSESSIONAL CONSULTATION OF THE *AD HOC* COMMITTEE DEDICATED TO MULTI-STAKEHOLDERS

On the 24th and 25th of March 2022, the first Intersessional Consultation of the *Ad Hoc* Committee, dedicated to multi-stakeholders, to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies (ICT) for Criminal Purposes was held in Vienna.

The meetings had been called by the Chair of the *Ad Hoc* Committee, H.E. Ms. Faouzia Boumaiza Mebarki, in accordance with General Assembly resolution 75/282[98].

Thanks to these reunions, multi-stakeholders – representatives from NGOs, global and regional intergovernmental organizations, and civil society – had the possibility

[98] UN General Assembly Resolution 75/282: Countering the use of information and communications technologies for criminal purposes

to provide to the Chair and Member States new ideas to consider for the elaboration of the new Convention.

As agreed previously on the agenda, the Intersessional Consultation dealt with three specific items: criminalization, general provisions, procedural measures and law enforcement.

Many themes arose in the discussion on criminalization, especially by Article 19, Access Now and Foundation for International Blockchain and Real Estate Expertise (Fibree Foundation), the three panelists that explained their panels before the *Ad Hoc* Committee.

More specifically, the attention was focused on the crucial role played by stakeholders for the realization of this Convention, because their expert competences may provide to Member States new perspectives and important elements to include within the Convention.

As already proposed during the First Session of the *Ad Hoc* Committee, these stakeholders were concentrated on fundamental rights and freedoms, especially stating how noteworthy is the impact of cybercrime on individuals.

In the light of what discussed herein among Non-Governmental Organizations, Member States and Civil Society, a particularly progressive aspect analyzed was about the balance between the defense from cybercrime and the necessity of a protection related to fundamental rights and freedoms, in detail the freedom of expression: despite the imminent collective need to protect/be protected by/from cybercrime, it could arise the risk to limit a person's freedom to express their own opinion legitimately, originating a counter-productive effect. References to UNTOC, UNCAC and Budapest Convention are necessary to maintain the same thread, so avoiding to repeat same disciplines, already protected by these Conventions.

The discussion on general provisions of the Convention had as panelists University For Peace and International Conference For Cyberlaw, Cybercrime and Cybersecurity, which suggested to create an harmonized system of rules and institutions to counter and combat cybercrime.

Moreover, the importance to attribute value to jurisprudential opinions was also stated.

Among different propositions, criminalization for aiding and abetting people to commit cybercrime was particularly highlighted: cybercrime is perpetrated by many authors generally, and for this reason it is necessary a regulation on aiding/abetting and also on cyber-organized crime.

An idea strongly appreciated by Member States was about the question of the "ambiguity" of terms: the importance of a technical terminology on cybercrime and ICTs had been affirmed also during the First Session of the *Ad Hoc* Committee; not by chance, even in this occasion, the subject was re-proposed, underlining the importance to remove possible ambiguities of words, which may cause difficulties for the interpretation. So, it is necessary to spread knowledge related to cybercrime regulations: despite the increasing of this crime is known worldwide, many people do not know really how cybercrime acts. Stakeholders proposed the circulation of information about it, informing directly people on the effects, and trying to avoid a huge problem: becoming a criminal without even knowing it.

The last subject treated was about procedural measures and law enforcement, with INTERPOL, Privanova SAS, Microsoft and eLiberare Association as panelists.

During the discussion, it was underlined the fundamental role of INTERPOL, on the law enforcement phase, especially because judicial police is the body which handles immediately with the effects and consequences of crime. Indeed, one of the most well-liked proposal was on the application and implementation of coordinated operations among Member States, so improving cybersecurity, together with the help of corporations.

The presence of a colossal like Microsoft was particularly encouraging: even the most important corporations make efforts for a common cause, giving the instruments and means to counter and combat cybercrime.

The best solution remains international collaboration and cooperation among States: sharing experiences and electronic evidence, Member States may carry out incisive measures into cyberspace, without evading other states' sovereignty.

From these interactive dialogues among Member States and stakeholders arose stimulating ideas and suggestions, to include in the process of elaboration of the new Convention, which objective is to become a guidance for preventing and combatting cybercrime.

2.4 THE SECOND SESSION OF THE *AD HOC* COMMITTEE

The Second Session of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes was held in Vienna, from 30th May to 10th June 2022.

In accordance with the "Provisional Agenda", after the opening of the session, the Chair Boumaiza Mebarki presented the report on the first intersessional consultation with multi-stakeholders, specifying the importance of statements made by the NGOs, civil society, academia and the private sector in order to guarantee interactive dialogues with Member States, suggesting ideas to include in the new convention.

The main themes discussed during this second session of the *Ad Hoc* Committee were: provisions on criminalization, general provisions and provisions on procedural measures and law enforcement. Indeed, they represent the core of this new convention against cybercrime. For this reason, in order to avoid the possibility to conduct a rough and coarse process of negotiation, the Chair had theorized an inclusive method to participate to the debate, creating some questions to submit to Member States about the topics to deal with.

Starting from the provisions on criminalization, in order to avoid that some types of crimes could not be treated very well, the Chair preferred to divide the subject in five groups[99].

The first group concerns cyber-dependent crimes, such as illegal, unlawful and unauthorized access, interference of data and systems, obstruction of computer programs, misuse of devices or malicious software and so on. The debate examined the question of *mens rea* in a very punctual manner, underlining the intentional nature of these kind of offences. In relation to the specific conducts perpetrated, the concept of harm was analyzed: according to some States it should occur, but for the most part of delegates it is not necessary that a serious and material harm occurs in order to constitute the crime; for this reason, it was suggested to consider the concept of harm as an aggravating circumstance.

[99] See "Letters from the Chair of the *Ad Hoc* Committee, including guiding questions" in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

Also, the attempt to commit cyber-dependent crime should be criminalized, for having endangered systems or confidential information.

A very debated topic which brought to a common perspective was on the inclusion of wide definitions, avoiding restrictive ones which may limit the range of actions of the legislative provisions. It was suggested to "not itemize" crimes.

The infringement of security measures was analyzed in relation to its nature, whether it is a crime or a simple circumstance.

And at last, a recurring theme was cyber-attacks to infrastructures, which should be considered an aggravating circumstance, according to the majority of delegates.

The second group of questions proposed by the Chair focused on identity-related offences, fraud, forgery and infringement of copyright. The discussion concerned mostly the feature of fraud, perpetrated entirely or partially through the use of ICTs, and whether it could be considered a broad offence that may cover other conducts like theft, scam, financial offences and electronic payment tools offences. Points of view were conflicting: on the one hand, a lot of Member States considered worthwhile fraud to cover other crimes, because various manifestations of it; on the other hand, some delegates preferred to distinguish all types of offences, since they are based on different requirements.

Another important crime, forgery, committed fully or in part online, was debated, especially in relation to its dangerousness, and whether it may contain other criminal conducts, for instance creation of information to mislead users.

Even for this group of offences, the theme of mental element was affirmed, agreeing on intent.

Identity-related offences were taken into account during the discussion because of their content, related to sensitive data and confidential information: many delegates would prefer to distinguish identity theft from other conducts as the use of personal data to commit crimes. But in general, the most part of Member States agreed on the inclusion of these topics in the new convention.

The violation of copyright was considered not necessary to be provided for, not only because this matter is already disciplined by other regional and international instruments, but also because copyright is covered by domestic law mainly.

Questions related to the third group concerned mostly online child sexual abuse, child sexual extortion, revenge porn, violation of privacy, involvement of minors in the commission of illegal acts.

Premising that minors must have maximum protection, because of their vulnerabilities and exposition to the risks of the Internet, according to some delegates it is preferable to use the age parameters indicated in the Convention on the Rights of the Child, in order to guarantee an extended safeguard. Moreover, the Budapest Convention together with the Lanzarote Convention could be good point of reference to elaborate disciplines of the new UN legal instrument.

Production, diffusion, selling of child sexual material is inevitably punishable. Member States debated also on the penalization of mere access and viewing child sexual abuse material, and whether these conducts should be considered crimes (consisting in the prelude of more serious offences) or not.

Some of the most popular practices of the last few years, online grooming and revenge porn, should be defined and disciplined into the convention.

And finally, child sexual extortion and exploitation should be taken into account, because harmful conducts: children are not mature enough to understand what is happening, especially if they are under the age to express the sexual consent. For this reason, Member States suggested to define all of these behaviors in a very flexible way, to cover as many connotations as possible.

As it was already explained in this thesis, these kinds of sexual practices have a strong impact on children and their psychological developments. Very often, suicidal intentions are reached once these people become aware of the injuries suffered. But, many Member States agreed on the exclusion of crimes related to encouragement to suicide.

The last two groups of questions proposed by the Chair on respectively terrorism-related offences, offences related to discrimination, racism, xenophobia, distribution of narcotic drugs, arms trafficking and organized crime (fourth group) and money laundering, aiding, abetting, participating in, attempt, obstruction of justice (fifth group) were discussed together.

The debate on these two groups was the most controversial one of the criminalization item: on the one hand, a lot of Member States proposed to not

include in the new convention offences related to discrimination, racism, arms and drugs trafficking because there could be the risk to go off-topic, and besides they are already disciplined by other international conventions; on the other hand, some delegates strongly supported the addition of such themes, since these phenomena are increasing steeply through the use of ICTs.

There are conflicting opinions on terrorism-related offences, even if the majority of delegates tended to include them, especially for cyber-terrorism.

Participation in, aiding, abetting and attempt were considered by some Member States relevant for the future convention, although others suggested a domestic discipline. The most part of delegates agreed on the inclusion of money laundering, especially in its cyber manifestation.

The only question approved by everyone was on the extension of the criminal liability to legal persons, consistently with the UNTOC provisions.

The discussion about general provisions dealt with a lot of matters.

Indeed, besides some general indications on purposes and scope of the convention, the importance to use technological neutral language within the text was underlined, thus without specifying all ICTs which can be used to commit a crime, or there could be the risk to limit the range of action of this convention, becoming useless for the future. Instead, the technology neutral approach would adapt to the constant evolution and development of ICTs.

Moreover, using terminology similar to the previous conventions UNTOC and UNCAC is appropriate to maintain the same narrative thread. Both of them are true models to follow, especially in reference to the structure of the convention.

Delegates stressed a lot on the respect of the principle of sovereignty, legality and proportionality.

Furthermore, Member States were in favor of using electronic evidence, which should not be limited to the offences indicated into this new international legal document, but also to other crimes, in order to spread practice to use.

The presence of a discipline on human right was debated too: the most part of Member States preferred to provide for provisions dedicated to fundamental rights and freedoms, but others stressed on the point that this convention is aimed to crime prevention, and not on human rights. Thus, a protection should be contemplated,

with more emphasis on freedom of expression and right to privacy. Furthermore, delegates restated the importance to take into consideration gender perspective, making a balance between abstract provisions and phenomenology.

Private Sector and NGOs had the opportunity to have the floor and express their opinions on general provisions: more specifically they underlined that the principle of sovereignty is not the point of the convention, which instead it is international collaboration among countries and also multi-stakeholder, in order to harmonize the international legal framework. Moreover, they stressed on the inclusion on specific protections of human rights and right to privacy.

Just like in the scope of criminalization, the Chair preferred to divide the item of procedural measures in four groups, to deal with the aforementioned topic in detail[100].

The first group of questions proposed focused on general aspects such as issues that may arise on jurisdiction, because of the borderless/cross-border nature of cyberspace. Among the criteria to include in the convention to determine the jurisdiction, Member States opted for the targeted State one.

Procedural measures and law enforcement provisions should not be applied only in reference to the crimes specifically provided for by the convention, but also to other offences, in view of the constant evolution of cybercrime. In the application of such measures, it would be appropriate to follow principles of necessity, proportionality and sovereignty of States. As the Argentina's distinguished delegate said "even if cyberspace is trans-border, this is not a justification for infringing the principle of state sovereignty".

According to Member States, within the chapter on procedural measures there should be also disciplines on electronic evidence, investigative tools and techniques.

The second group of questions proposed by the Chair analyzed the specific procedural measures to be applied. The well-liked ones were: collection of information and meta data transmitted by means of ICTs; information stored or stored computer data; real-time collection of traffic data; expedited preservation of

[100] See "Letters from the Chair of the *Ad Hoc* Committee, including guiding questions" in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

stored computer data; production orders; search and seizure. Delegates proposed also to add measures already provided in other international instruments. References to the Budapest Convention were a lot, more specifically to its classification of data, suggested again herein, which distinguish subscriber ones, traffic ones and content ones: subscriber data means any information held by a service provider, relating to subscribers of its service, which concern subscriber's identity, address, access or telephone number and so on; traffic data means any computer data generated by a computer system, indicating the communication's origin, destination, route, time, date etc.; content data means any data that conveys the meaning or substance of a communication as well as data processed, stored, transmitted by computer programs.

As it was affirmed before, the respect for principles of proportionality and necessity is fundamental in order to apply procedural measures in a proper and legitimate way.

The third and the fourth groups of questions were discussed together, and the debate reached a commonly agreed line on those specific disciplines to include in the chapter dedicated to procedural measures and law enforcement. In particular, the majority of Member States agreed on the addition of provisions on freezing, seizure and confiscations, recalling disciplines provided in the law of reference, which is UNTOC.

There was no opposition even for provisions on specific protections for witnesses and victims of cybercrime.

Instead, differing opinions were stated on the modalities of regulations of digital evidence, despite the most part of Member States expressed a preference for dealing with this topic generally, consenting to domestic legal systems to discipline admissibility and technical aspects.

Delegates agreed on the inclusion of provisions on establishment of criminal record, measures to enhance collaboration with law enforcement authorities and special investigative techniques, recalling disciplines provided for by UNTOC, in order to maintain compliance with the other international instruments.

On the theme of procedural measures and law enforcement multi-stakeholders intervened also, which reaffirmed the importance of the collaboration between private sector, NGOs, intergovernmental organizations and Member States.
Although the success reached by the Second Session of the *Ad Hoc* Committee, differences of expressed opinions did not allow the formation of a common orientation, especially on the criminalization. On the one hand, Western States, many Latin American and Caribbean States, as well as Japan, South Korea, Nigeria and South Africa prefer to focus more on cyber-dependent crimes, significantly increasing, compared to traditional crimes which can be perpetrated through the use of ICTs, with exception of online child sexual exploitation; on the other hand, countries like the Russian Federation, China expressed a strong will to include cyber-enabled crimes is shown, mostly for those conducts which involve terrorism, hate speech, drug trafficking and economic-related offences[101].
Also, different points of view were spoken up in regard to the regulation of procedural measures, with some delegates who would prefer a detailed discipline, and others who would opt for simple guidelines, allowing domestic legal systems to analyze the matter according to their national rules.
The purpose of the *Ad Hoc* Committee for the next sessions is to strike a balance between different necessities, taking into account all of them, in order to reach the consensus.

2.5 THE SECOND INTERSESSIONAL CONSULTATION OF THE *AD HOC* COMMITTEE DEDICATED TO MULTI-STAKEHOLDERS

On the 13th and 14th of June 2022, the Second Intersessional Consultation of the *Ad Hoc* Committee, dedicated to multi-stakeholders, to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, was held in Vienna.
As for the first Intersessional Consultation, multi-stakeholders had the possibility to present and propose new suggestions concerning the items to include within the

[101] I. TENNANT, S. WALKER, *Under the microscope: Delegates get into the details as UN cybercrime negotiation move forward*, Global Initiative against Transnational Organized Crime, Vienna, 2022

new convention against cybercrime. The work organization followed the same method adopted in March, so discussions conducted by panelists mainly, with interventions by other NGOs, civil society and academia.

The meetings dealt with matters which will be analyzed at the Third Session of the *Ad Hoc* Committee, which are: international cooperation, technical assistance, preventive measures, mechanism of implementation, final provisions and preamble. Each topic was examined with attention by panelists, who presented their observations on the basis of what emerged during the previous sessions, and also based upon their direct experience with the cybercrime phenomenon.

Starting from the debate on international cooperation, the first panelist was Microsoft Corporation, which restated once again the importance of the presence of multi-stakeholders in the negotiating phase of this new convention. It also underlined the importance of the Budapest Convention together with its Second Additional Protocol as models, especially about international collaboration and divulgation of electronic evidence. The relevance of international collaboration between Member States and the private sector was highlighted, especially for addressing cybersecurity and disinformation threats. The creation of partnerships also among corporations could be useful for the purpose of interoperability: the ability of different systems, devices, applications or products to connect and communicate in a coordinated way, without effort from the end user. Functions of interoperable components include data access, data transmission and cross-organizational collaboration regardless of its developer or origin[102].

International Center For Criminal Law Reform and Criminal Justice Police affirmed how much the world has changed after the advent of information and communications technologies, and for this reason, a punctual regulation against cybercrime is necessary. Member States should characterize precise techniques, applicable at global level.

UNTOC and UNCAC are examples to follow, mostly for the methods related to international cooperation, in order to avoid damage to human rights. Therefore, mechanisms of mutual legal assistance are fundamental to create a valid

[102] See Microsoft Corporation's Panel presented at the Second Intersessional Consultation in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/2nd-intersessional-consultation.html

collaboration, together with trust, not only among States to share information, experience and practices, but also with private sector, which has technical competences on digital world.

Forum of Incident Response and Security Teams, also known as FIRST, aspires to bring together incident response and security teams, in order to improve law enforcement.

People should be informed about the risks they may bump into when using ICTs, so that they could act with greater conviction.

Policy and governance should collaborate to guarantee the elaboration of practices and laws against cybercrime, identifying also some sections of law enforcement specialized in digital environment[103].

The University of West Attica based its panel entirely on Artificial Intelligence, which should be improved more. In the last few years, digital criminality and online delinquency spread a lot: cybercrime is considered by everyone an issue which must be solved. It has to do with "behaviors without fatherland", damaging the world. For this reason, the aforementioned university proposed to use Artificial Intelligence for good purposes, even if generally it is used by cybercriminals to perpetrate crimes and infringe the barriers of security measures. A regulation on AI should be based on certain guidelines: it should be lawful, ethical, so respecting principles and values, and robust. To facilitate the elaboration of a discipline, the European approach on Artificial Intelligence should be taken into account by the United Nations, thus creating also a new aspect linked to the use of ICTs.

The ICC UK/World Business Organization focused on the importance of trust among States and also with private sector. Measures to counter cybercrime should be elaborated not only by countries or public organizations, but also those belonging to private sector who knows better the effects caused by cybercrime, having specific technical competences, useable to create new instruments to combat this phenomenon. It is necessary to limit as much as possible the impact of cybercrime on productivity, society and obviously individuals.

[103] See FIRST's Panel presented at the Second Intersessional Consultation in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/2nd-intersessional-consultation.html

In addition, INTERPOL presented an intervention on international cooperation, especially on how important is collaboration between law enforcement authorities. Such relations should aim to secure digital evidence and other forms of investigatory measures.

Thanks to INTERPOL Global Cybercrime Program, established some years ago, it is possible to help Member States to prevent, detect, investigate and disrupt cybercrime.

A key component is the regional cybercrime operational desks that provide Member States with support tailored to their local context, needs and challenges.

Boasting cybersecurity experts, INTERPOL allows dynamic communications to discuss with law enforcement authorities on prevention strategies, detection technologies and investigation techniques[104].

The panels related to the theme of technical assistance were preceded by a contribution from a representative of UNODC Global Programme on Cybercrime, which exposed in a very detailed manner the objectives to reach, for instance awareness of the phenomenon, specialized frameworks, joint operations, cooperation, public-private alliance, in order to aspire to the fulfillment of the 16th Sustainable Development Goal (Peace, Justice and Strong Institutions). The representative of the Global Programme affirmed also the importance of some instruments created by the UNODC, such as the SHERLOC portal, or the Digest on Cyber-Organized Crime, which should be taken into consideration in the elaboration of the new convention[105].

Once again INTERPOL had the floor to express the relevance of capacity building of law enforcement in single States. An international action could be considered valid if domestic instruments work too. Collaboration with private sector is crucial to create new devices and means, usable both for investigation and the procedural phase, providing for an effective system on electronic evidence.

---

[104] See INTERPOL's Panel presented at the Second Intersessional Consultation in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/2nd-intersessional-consultation.html

[105] See UNODC Global Programme on Cybercrime's Panel presented at the Second Intersessional Consultation in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/2nd-intersessional-consultation.html

Ohaha Family Foundation recalled the global crisis caused by the Covid-19 pandemic, underlining that developments stopped as well as the world did.
Everything became more and more digitalized, and ICTs became essential in everyday life, bringing about a change in criminality too. For these reasons, international cooperation is fundamental to move forward, involving both developed countries and developing ones in.
Training common people could be useful to at least mitigate effects and expansion of cybercrime, together with also the development of innovative technologies by corporations.
Cybersecurity Tech Accord focused its panel on the improvement of techniques used by cybercriminals to commit crimes: sophisticated techniques such as anonymity, the use of dark web. Technical assistance is essential as well as capacity building, in order to provide instruments to combat cybercrime. This type of offence endangers common people and private sector mostly, not only organizations and public institutions. Thus, the collaboration with experts of private sector is fundamental, since they know strategies to apply against cybercrime.
The United Nations International Computing Centre (UNICC) recalled some objectives in common with the work of the *Ad Hoc* Committee: identifying innovative, cost effective and resilient cybersecurity solutions. A reference was made about the United Nations Joint Inspection Unit recommendation to build a fund and encourage Member States to contribute to it. In 2021, the UNJIU, an independent external oversight body that conducts evaluations, inspections and investigations in the UN, reviewed the use of cybersecurity practices across the UN, with distinct recommendations for UN Agencies to leverage cybersecurity services from the UNICC. The JIU report identifies common cybersecurity challenges and risks faced by the UN system, provides an analysis of responses to these threats and examines current dynamics as well as the potential for shared solutions[106].
During the general debate on technical assistance between panelists and the other multi-stakeholders, a discussion arose on the use of dark web for investigations, adopting strategies with respect of legality. Despite some limitations since the dark

[106] See UNICC's Panel presented at the Second Intersessional Consultation in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/2nd-intersessional-consultation.html

web is unknown to those people who navigate on the Internet legally, exploring this part of cyberspace could be beneficial to understand the methods used by cybercriminals to exchange information. In general, stakeholders promote an open and safe space on the Internet.

Panels presented on preventive measures analyzed cybercrime, identifying those modalities to intervene before the crime is occurred.

According to International Chamber of Commerce (ICC), the first step to achieve a correct prevention is awareness: informing communities and individuals of the risks of this offence. Partnerships with private sector, collaboration with civil society and academia, are fundamental to spread knowledge on this phenomenon. Besides them, supporting capacity building, training for investigators, education at all levels could be efficient[107].

The Inter-Parliamentary Union highlighted the increase of dependence from ICTs, so the necessity to build a global culture on cybersecurity, through partnerships and coordinated efforts with the society.

In detail, investing on cybersecurity may bring to technological developments, with the aim to establish a safe digital environment. International coordination should not be restricted to the legal aspects, like the elaboration of a new convention, but also to those preventive and defensive measures to implement, in order to counter cybercrime. Exchanging techniques and strategies could constitute a good foundation for an incisive international collaboration.

The Inter-Parliamentary Union suggested to involve parliaments in the negotiation of the new convention, not only because as public institutions they are targets for cyber-attacks, but also because they may strengthen communications among States and citizens.

Moreover, the aforementioned global organization recalled the importance of INTERPOL to coordinate actions and assist victims.

A1 Telekom Austria identified DDos attacks, phishing and smishing, the use of malwares as main cyber threats. For this reason, it is necessary to enhance protections and performances of systems and websites, so that they may recognize

[107] See International Chamber of Commerce's Panel presented at the Second Intersessional Consultation in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/intersessional-consultations/2nd-intersessional-consultation.html

automatically a real or fictional e-mail, or SMS. For instance, in case of smishing perpetrated through the malware Flubot, the infection starts from an SMS, apparently innocuous but actually fraudulent, which contains fake contents and links, that if clicked, they lead to requests to data. Once these data are inserted, generally they are stolen, causing account thefts.

The last discussion of this Second Intersessional Consultation dealt with provisions for mechanism of implementation, final provisions and preamble.

The first panelist, Association pour l'integration et le developpement durable au Burundi, underlined the importance of the role of civil society and indigenous peoples' organizations in the process of implementation of the convention. Indeed, they may show and make understand to national parliaments the elaboration of this new convention, in order to improve cybersecurity.

The Alliance of NGOs on Crime Prevention and Criminal Justice focused on review mechanisms, essential to assist Member States for the correct implementation of international conventions.

UNTOC and UNCAC are the foundations, not only for the review mechanisms but mostly for the implementation of them at national level, guaranteeing the application of these incisive disciplines.

Thus closes the Second Intersessional Consultation dedicated to multi-stakeholders to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. The meetings of the Third Session of the *Ad Hoc* Committee will be held again in New York, from 29th August to 9th September 2022.

2.6 CONTEXTUAL DEVELOPMENTS TO THE NEW CONVENTION ON CYBERCRIME

Simultaneously to the process of the elaboration of the new convention on cybercrime, at its tenth session in October 2020, the Conference of the Parties to the United Nations Convention against Transnational Organized Crime adopted Resolution 10/4 (Falcone Resolution), through which it requested the UNODC to provide technical assistance and capacity building to Member States and support their efforts for the fight against transnational organized crime *so including "the updating, as necessary, of model instruments and publications, such as the guide*

on current practices in electronic surveillance in the investigation of serious and organized crime developed by the United Nations Office on Drugs and Crime in 2009, [and] the model law on mutual assistance in criminal matters developed by the Office in 2007 […] with a view, as appropriate, to including provisions and updated material on the use of special investigative techniques and the gathering of electronic evidence" [108].

UNODC held two informal expert group meetings in 2021 to update the Model Law on Mutual Assistance in Criminal Matters (2007). These informal expert group meetings were funded by the Government of Japan and the United Kingdom. The revised Model Law on Mutual Assistance in Criminal Matters, as amended with provisions on electronic evidence and the use of special investigative techniques, is brought to the attention of the Commission on Crime Prevention and Criminal Justice to inform Member States and also to consider the discussion on "strengthening the use of digital evidence in criminal justice and countering cybercrime, including the abuse and exploitation of minors in illegal activities with the use of the Internet". In detail, the updated version of this document together with the 2022 Model Legislative Provisions against Organized Crime formulated by the UNODC include new model legislative provisions on undercover investigations, electronic surveillance and assistance to and protection of victims. One emerging issue is the collection, use and admissibility of electronic evidence in criminal proceedings, as they could conflict with the principle of legality, as well as with the typical principles for protection of fundamental rights and freedoms.

Electronic evidence is any probative information stored or transmitted in digital form, such as photos, videos, audios or IT documents, which are contained within cyberspace. The collection, use and admissibility of such information requires legislation beyond the model law provisions proposed. This may also involve the storage and preservation of data, and the real-time collection of such data. To face the challenges related to electronic evidence and its international dimension and to give law enforcement, judicial authorities adequate tools to address them, adapting

[108] "Model Law on Mutual Assistance in Criminal Matters (2007), as amended with provisions on electronic evidence and the use of special investigative techniques (2022)" elaborated by the Commission on Crime Prevention and Criminal Justice

domestic laws and international cooperation measures. Such tools must, however, be subjected to strong mechanisms for protecting fundamental rights and freedoms. Oversight of the use of special investigative techniques by judicial authorities is common practice in many jurisdictions, following international human rights law.
Electronic surveillance means the monitoring, interception, copying or manipulation of messages, data or signals transmitted by electronic means; it is only lawful if it has been authorized, and it could be very useful for facilitating investigations. Electronic surveillance in the form of listening devices or the interception of communications is often preferable where physical infiltration or surveillance would represent an unacceptable risk to the investigation or the safety of investigators. Given its intrusiveness, it is generally subject to strict judicial controls and numerous statutory safeguards to prevent abuse[109].
The issues related to these instruments concern the admissibility of them, linked to the principle of legality.
The aforementioned "Falcone Resolution", which pursues the implementation of the Palermo Convention, aims to promote an efficient use of special investigative techniques and the conclusion of international agreements that may facilitate cooperation through these practices. Cybercrime, and more in general the use of information and communications technologies for criminal purposes represent the sector to which some of the most important operational measures appear to be specifically related, thus joint investigative bodies use modern technologies, agreements for the use of special investigative techniques (and, in particular, electronic surveillance) in transnational investigations, as well as cooperation between public authorities and communication service providers[110].
The Falcone Resolution, the content of the Model Law on Mutual Assistance in Criminal Matters and the latest Model Legislative Provisions against Organized Crime show the importance of disciplines on electronic evidence and surveillance, the latter considered the future of criminal law. Despite being soft-law regulations, so not actually binding, they have a universal efficacy, since a real and effective

[109] UNODC, *Model Legislative Provisions against Organized Crime*, Second Edition, Vienna, 2021
[110] A. BALSAMO, A. MATTARELLA, *Criminalità organizzata: le nuove prospettive della normativa europea*, Sistema Penale, 2021

problem is encountered, seeking greater incisiveness. The purpose of these instruments is to create a harmonization of norms on digital evidence and electronic surveillance, achievable only through a collaboration among countries of the world, taking into account also the protection of the right to privacy, inevitably damaged. These soft-law regulations aim to spread practices to use these means.

CHAPTER 3

THE COMMITMENT OF MULTI-STAKEHOLDERS IN THE *AD HOC* COMMITTEE

SUMMARY: 3.1 The Importance of the Participation of Multi-Stakeholders and Civil Society in Decision-Making Processes – 3.2 Theories and Submissions from Multi-Stakeholders related to the sessions of the *Ad Hoc* Committee – 3.3 State of Play and Future Perspectives of the *Ad Hoc* Committee

3.1 THE IMPORTANCE OF THE PARTICIPATION OF MULTI-STAKEHOLDERS AND CIVIL SOCIETY IN DECISION-MAKING PROCESSES

The presence of multi-stakeholders in decision-making processes guarantees the possibility to understand the phenomenology of events: indeed, these groups express and show their field experience, pursuing for the elaboration of new instruments and solutions which could be appropriate to fight harmful conducts.
The category of multi-stakeholders includes non-governmental organizations, civil society, academia and private sector, who are essential in devising viable solutions since they are often among the frontline victims of crime, both directly and indirectly. They provide first-hand views on crime, real and perceived, while offering a way out to deal with these, both at the grassroot and global level[111].
Multi-stakeholders have been actively working towards the implementation of legislative documents through projects, researches, initiatives, advocacy, knowledge-sharing and monitoring, indeed they can reach the wider audience and achieve effective results on various levels[112].
In the course of time, the importance of these bodies has increased so much, and for this reason the United Nations involves them in committees and conferences, in order to take into account new suggestions and ideas not considered before. Moreover, multi-stakeholders' relations can enable the early identification of risks

[111] UNODC, GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME, *Guide for civil society community engagement with the UNTOC Review Mechanism*, Vienna, 2020
[112] See www.unodc.org

and opportunities, and therefore the implementation of sustainability measures that contribute to initiatives.

Not by chance, the UN has recognized the importance of the role played by multi-stakeholders also for the implementation of the seventeen Sustainable Development Goals of the 2030 Agenda.

More specifically, the 17th SDG on "strengthen the means of implementation and revitalize the Global Partnership for Sustainable Development" recognizes multi-stakeholder partnerships as important vehicles for mobilizing and sharing knowledge, expertise, technologies and financial resources to support the achievement of the sustainable development goals in all countries, particularly in developing countries[113]. Goal 17 further seek to encourage and promote effective public-private and civil society partnerships, building on the experience and resourcing strategies of partnerships.

The importance of multi-stakeholders has been recognized also by the UNODC. Indeed, this organ decided to include them in the process of elaboration of the UN Convention against Corruption, albeit to a limited extent, and then in the Review Mechanism of the UN Convention against Transnational Organized Crime. In these occasions, multi-stakeholders contributed to strengthen capacity building and reach a successful implementation of the conventions, conducting constructive dialogues. Indeed, an online knowledge hub called "Whatson" was created for NGOs, private sector and academics to counter organized crime and corruption, exchanging and sharing information and operations contrasting these two phenomena.

Besides the references to the generic concept of "multi-stakeholders", the United Nations often recalls the relations with non-governmental organizations, in accordance with article 71 of the Charter, which allows the possibility that NGOs can be consulted by the Economic and Social Council, recalling also the ECOSOC resolution 1996/31 on "Consultative Relationship between the United Nations and Non-Governmental Organizations"[114]. In addition, the UN aims to build strong and efficient relations with the entire category of "civil society", referred as the third

[113] See www.unodc.org

[114] ECOSOC Resolution 1996/31: Consultative relationship between the United Nations and non-governmental organizations

sector alongside governments and private businesses[115]. The World Bank has adopted a definition of civil society developed by a number of leading researches centres: the term civil society is to refer to "the wide array of non-governmental and not-for-profit organizations that have a presence in public life, expressing the interests and values of their members or others, based on ethical, cultural, political, scientific, religious or philanthropic considerations"[116]. Indeed, civil society expresses the interests of social groups and raises awareness of key issues in order to influence policy and decision-making. In recent decades, Civil Society Organizations (CSOs) have been successful in shaping global policy through advocacy campaigns and mobilization of people and resources[117].

The members of civil society promote the same interests, purposes and values pursued by the United Nations: fight poverty, corruption, economic inequalities, cope with humanitarian crises, protect the environment, fight all forms of discrimination, prevent crime.

The participation to decision-making processes involves the freedom of expression of representatives, who may act freely and promote different positions expressed by other authorities. But acting in the public interest requires openness, clarity, transparency and accountability of public officials to citizens.

Moreover, the current UN Secretary-General Antonio Guterres said "Civil society is a key instrument for the success of today's United Nations where governments are finding it more and more difficult to do their job. […] Dialogue and cooperation with civil society will, I'm sure, be a central aspect of the activities of the United Nations in the next few years, not only because of my own activities, but because of the concerns that all the United Nations bodies have, making sure that partnership becomes a key element in solving global problems".

UNODC recognizes the need to promote strong partnerships and an active involvement with civil society organizations. UNODC Civil Society Unit (CSU) is the main entry point for non-governmental stakeholders and serves as a bridge

[115] See http://www.un.org/en/sections/resources-different-audiences/civil-society/ on civil society in the UN

[116] World Bank, Civil society, https://www.worldbank.org/en/about/partners/civil-society/overview

[117] G. SGUEO, *La società civile nell'Organizzazione delle Nazioni Unite*, www.diritto.it, 2008

between these stakeholders and UNODC substantive offices, field offices and the Member States[118].

The objective of civil society in UNODC is to increase non-governmental stakeholder engagement in the implementation of the conventions falling under UNODC's mandates, and to enable stakeholders to promote their implementation at global, regional, national and local levels. As such, UNODC recognizes the need to promote strong partnerships with CSOs in dealing with the complex issues of drug abuse, corruption and in general crime.

As it was already said, the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is composed of delegates of the 144 participating Member States, Observers, members of the United Nations Secretariat, representatives of global and regional intergovernmental organizations, including representatives of UN bodies, specialized agencies and funds, as well as representatives of functional commissions of the Economic and Social Council, representatives of non-governmental organizations that are in consultative status with the Economic and Social Council, in accordance with the Council, representatives of other relevant non-governmental organizations, civil society organizations, academic institutions and private sector[119].

In this specific case of the aforementioned *Ad Hoc* Committee, the inclusion of civil society is not accidental, but it is the result of years of collaboration, which has brought benefits for the implementation of international instruments such as UNTOC and UNCAC.

For this reason, along with the active participation to regular sessions of the *Ad Hoc* Committee, the Chair opted to hold intersessional consultations dedicated to multi-stakeholders, in order to guarantee to members of NGOs, civil society, academia and private sector to express about the matter in hand. In this specific case, their contribution is not limited to the implementation of the future convention, but it refers to the process of elaboration of it, since they may provide suggestions and proposals to include, which could not be considered by the other participants

[118] See www.unodc.org on UNODC Engagement with civil society on drugs and crime

[119] UN General Assembly Resolution 75/282: Countering the use of information and communications technologies for criminal purposes

before; they may illustrate records about damage caused by cybercrime, underlining some points deserving relevance; they may suggest techniques to adopt. Within these groups, many experts on cybercrime, cybersecurity and in general cyberspace are present, providing new methods to counter this offence, recommending disciplines, instruments and the use of ICTs for positive purposes.

3.2 THEORIES AND SUBMISSIONS FROM MULTI-STAKEHOLDERS RELATED TO THE SESSIONS OF THE *AD HOC* COMMITTEE

In the light of what emerged from the *Ad Hoc* Committee's Sessions and Intersessional Consultations dedicated to multi-stakeholders, cybercrime is perceived by States of the world and more as a transnational threat, hard to counter. The arrival of the Internet, and thus also the digital era, determine a true change of the physiognomy of criminality: the modalities used to bring about activities related to cybercrime has evolved increasingly, on the basis of the constant development of ICTs. In this moment, predictions estimate that offences perpetrated in cyberspace will increase significantly, if contrasting measures are not implemented immediately to mitigate its effects.

This offence has involved in every type of legal subject: countries, international organizations, private sector and also citizens. Cybercriminals act for several purposes: to weaken governments, to disable websites or to target single persons.

Contextualizing the crime under consideration in a precise category is not easy, mostly for its various manifestations in cyber-dependent crimes and cyber-enabled crimes.

Threats are several and dynamic: cybercriminals exploit cryptography, cryptocurrencies and anonymity to act undisturbed, conducting operations of any kind. Besides financial crimes and cyber-terrorism, their activities damage also individuals, such as trafficking in human beings, smuggling of migrants, child sexual exploitation. Even though they are spread in the whole world, these specific manifestations of traditional crimes could be countered through actualized domestic legislations. The real and main issue consists in cyber-attacks entirely conducted in

the digital dimension, which could cause violations of privacy and crimes related to personal and sensitive data.

Given the scale of the challenges, the only method for countering this phenomenon is international collaboration and cross-border operations: these offences are not just a matter of non-localized crimes, but above all non-material ones. In fact, sometimes a material harm or damage does not occur, some people find out the occurrence of the crime too late.

Cooperation among countries of the world is essential, guaranteeing new rules of law, and cybersecurity instruments for protection and prevention, taking into account fundamental rights, and balancing them with the necessities arisen from this phenomenon.

For these reasons, a new global convention formulated by the United Nations is found to be necessary, as well as it was for organized crime and corruption, which have UNTOC and UNCAC respectively. Other international and regional legislations are not enough to combat against this type of offence. Cybercrime is a transnational crime, and precisely because of this, it should be faced with a transnational contrasting action. The United Nations' work is the only which can mitigate this phenomenon, because of the vastness of its range of action. For this reason, the UN and its Member States agreed on the establishment of an *Ad Hoc* Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. Besides formulating a new global document alongside UNTOC and UNCAC, this organ wants to study the criminal conduct as much as possible, in order to provide incisive and accurate measures.

Moreover, the real aim of this new universal legal instrument is to reach international cooperation, the only solution to address such a widespread offence, living in cyberspace. It is necessary that all Member States establish trustful relations, supporting each other, in order to reach an optimal convention for everyone. Therefore, Member States may encourage this trust, providing some practical tools to enhance technical assistance and build capacities, and promoting exchange of information, experience and good practices. These actions would allow

to strengthen friendly relationships and enhance others, avoiding eventual abuse of power.

The Convention should take into account the existing regional and international legal framework, especially the Budapest Convention on cybercrime, and the two UN Conventions UNTOC and UNCAC. As well-structured documents, they could be good foundations which may give causes for reflection, avoiding the possible duplication of them.

One of the main purposes of this convention should be the protection of human rights and fundamental freedom, balancing them with a punctual and incisive discipline on countering cybercrime, and more in general the use of information and communications technologies for criminal purposes. All fundamental principles indicated in the UN Charter must be respected, to guarantee consistency and protection for both Member States and individuals.

As regards the scope, this new UN convention should create new substantive and procedural provisions, together with disciplines regulating international cooperation and mechanism on implementation.

In order to elaborate an accurate and clear convention, definitions of terms should be included to determine the content of the convention, using terminology already agreed in existing international texts. In this specific context, technological neutral language would be useful to cover not only offences perpetrated with the existing ICTs, but also with future ones.

Substantive criminal law provisions should criminalize both cyber-dependent crimes and cyber-enabled crimes for reaching an open, free and stable cyberspace, respecting human rights.

In regard to the specific type of offences, the focus should be mostly on cyber-dependent crimes such as unauthorized access or misuse of devices and malicious software, as still disciplined in an incomplete manner; the inclusion within the convention cyber-enabled crimes should be contemplated too, especially for the most spread and serious ones, like terrorism, fraud, forgery, child sexual exploitation and abuse. For sure, in the convention, disciplines on all already existent crimes eventually perpetrated through the use of ICTs cannot be present, but the future rules could provide for an extension to them.

In addition, provisions on criminalization should include disciplines related to criminal liability and mental element of the authors of the crimes.

General provisions of the convention should contain dispositions on the purpose and scope, jurisdiction, discipline about the protection of human rights and fundamental freedoms, taking into account that the present convention is not a human right document. The inclusion of guarantees of fundamental rights and freedoms should be contemplated, together with protections of victims, however considering the real focus of the convention, which is cybercrime.

Procedural provisions should include all measures such as confiscation, search, seizure which may mitigate the effects and consequences of the crime perpetrated. Moreover, disciplines on jurisdiction criteria may be useful, in order to avoid that more than one State could boast competences toward the same offence.

Procedural provisions have also to be in compliance with principles of legality, necessity, proportionality, and right to privacy, personal data protection, freedom of expression. Sometimes, these principles and rights collide, for instance in case of the application of restrictive measures and the right to privacy. For this reason, a balance should be struck, providing for the needs of everyone.

As other soft-law instruments already existent, this convention should encourage the use of electronic evidence and surveillance: in particular, in some States, national investigative powers involve disciplines related to electronic evidence, for example inspections of data or collection of files. And yet, other States have regulations which can be considered inadequate compared to modern times. Therefore, it is necessary to include in the new convention a discipline which may uniform this aspect, taking into account rules on the admissibility of evidence provided for by domestic legal systems.

Joint operations are incisive methods to combat cybercrime, which is extended all over the world, without any boundaries.

The convention should also include all mechanisms for cooperation and collaboration among Member States, especially in reference to investigations and prosecutions, considering also capacity building, sharing practices and experiences and also technical assistance, in order to guarantee to developing countries to participate actively to the fight against cybercrime. These practices allow the

development and building of trustful relations, which lead to an efficient collaboration.

Although good intentions are shown explicitly, the lack of transparency by some parts of States does not allow the formation of relationships of trust.

The latter is essential in order to obtain a successful cooperation, which can be reached only if international relations are characterized by equity and honesty[120].

The contribution given by multi-stakeholders, so non-governmental organizations, academia, civil society, private sector is fundamental for including experts' point of view. Indeed, they provide innovative suggestions and proposals to submit to Member States. Their collaboration means making common cause to combat this transnational phenomenon.

In order to understand clearly the contribution provided by multi-stakeholders, some submissions can be taken into consideration.

INTERPOL's contribution shows this intergovernmental organization has been receiving requests from Member States to address ransomware attacks against hospitals and other institutions on the front lines in the fight against the coronavirus.

In addition, cyber-frauds and data breaches continue to occur causing damage significant financial losses to businesses worldwide.

Cybercriminals are hard to find, because hiding in the dark web, that provides anonymity and untraceable access.

For this reason, the INTERPOL's objective is connecting police for a safer world.

"Its mandate is to facilitate cross-border law enforcement cooperation and, as appropriate, support governmental and intergovernmental organizations, authorities and services whose mission is to prevent or combat crime": reducing duplication of effort to optimize the use of existing mechanisms, channels and platforms in addressing cybercrime.

---

[120] A. MATTARELLA, *La futura Convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, Sistema Penale, 2022

«*In un'epoca in cui il cyberspazio è oggetto di contesa, il multilateralismo fatica a costruire fiducia tra i paesi. Data la mancanza di trasparenza che caratterizza l'opera di alcuni Stati nella lotta agli attacchi informatici, ci si è chiesti se essi vogliano realmente una convenzione che rischierebbe di evidenziare e punire determinate pratiche. Tuttavia, la gamma di minacce rivolte agli Stati ed ai cittadini induce a prefigurare un positivo esito degli sforzi messi in campo per la creazione di questo nuovo strumento normativo*»

Indeed, it can play a key role in the exchange of information, and the transmission of international cooperation requests. Its investigative support includes forensics, analysis, and assistance in locating fugitives around the world.

INTERPOL elaborated some strategic priorities and goals to combat cybercrime, for instance: enhancing international law enforcement cooperation for a timely and effective global response to cybercrime. Global information sharing and criminal data analysis are the cornerstone of all operational activity coordinated by INTERPOL.

Moreover, it proposes also the electronic mutual legal assistance (e-MLA) initiative to foster international cooperation in criminal matters by providing secure, electronic transmission capability for requests seeking judicial assistance in cross-border cases.

INTERPOL conducts strategic intelligence analysis of a specific crime threat or trend, or of criminal behavior in a particular environment. Based on this capability, INTERPOL develops global and regional assessments on cybercrime, which can make understand the development of threat landscapes and crime trends.

Another strategy elaborated is the delivery of capacity building projects and training courses to support member countries to enhance their cyber skills, knowledge and technical capabilities, and which are customized to their needs, in line with INTERPOL standards.

And finally, maximizing prevention efforts through public-private partnerships is one of the main activities which should be taken into consideration. Prevention of cybercrime requires participation by various stakeholders, including governments, law enforcement authorities, the private sector, international organizations, non-governmental organizations, academia, in addition to the general public. Countries should support businesses and communities in raising awareness of cybercrime risks, mitigation strategies and enhancing cyber hygiene, as these can have significant downstream preventive benefits. Partnerships based on trust within the global ecosystem of cybersecurity will be a deciding factor in formulating timely and effective response to cybercrime. In addition to the collaboration with private-

sector partners, INTERPOL plans to further engage with national cybersecurity agencies within INTERPOL's networks[121].

Besides INTERPOL, also Microsoft Corporation has manifested its interest toward the fight against cybercrime, since it is one of the main targets of cybercriminals. In its submission, this corporation underlines that the pivotal focus should be cyber-dependent crime, and its primary purpose should be to protect the targets and victims of cybercrime.

"The negotiation process will require full transparency and multi-stakeholder engagement if they are to be successful and any resulting treaty meaningful. Microsoft urges states engaging in the upcoming negotiations on a new cybercrime treaty to: pursue a systematic multi-stakeholder approach through meaningful inclusion and consideration of the equities of civil society, industry, academics, technical experts, and scientific and research institutions. They should be able to participate in the negotiations to the fullest extent possible.

The promotion of transparency should be guaranteed so that the negotiations are as open as possible. This includes the sharing of schedules, participants and draft texts, all of which should be made available to the public.

A new convention should encourage effective international cooperation between national law enforcement and prosecutorial agencies in investigating and prosecuting cybercrime: indeed, an opportunity for greater collaboration between governments and the private sector in matters related to lawful data access may lead to new strategies to combat cybercrime.

Moreover, the new convention should also provide a framework for capacity building to enable the effective investigation and prosecution of cybercrime globally, conducting consultations with the expert community. The creation of an expert forum that would allow states and participants from technical communities and industry to exchange views on the latest threats and potential mitigations would add to the security and stability of the online environment"[122].

[121] See the Submission formulated by the INTERPOL, published in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[122] See the Submission formulated by Microsoft Corporation, published in https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

Non-governmental organizations express their opinions underlining the importance to elaborate a new global convention on countering cybercrime, always taking into account their origins and main focus. Some NGOs are specialized on protection of children, others for peace, or fight against criminality.

For instance, Centro Studi e Iniziative Culturali Pio La Torre is an Italian non-governmental organization that is in consultative status with the Economic and Social Council, in accordance with Council. Its pivotal focus is to prevent organized crime phenomena, more specifically mafia ones, but also other crimes such as extortion and exploitation, and to provide assistance, solidarity and protection to victims, facilitating the growth of an "anti-mafia" mentality, both at national and international level.

Centro Pio La Torre submitted a contribution to the UNODC Secretariat, underlining the importance to include within the new convention references to the UNTOC, to continue a path already started. Moreover, the future international legal document should be focused on the protection of human rights and fundamental freedoms, especially those of the victims.

Centro Pio La Torre, particularly sensitive to the theme of organized crime, deems a specific section about cyber-organized crime should be included in the convention. Generally, cybercrime is perpetrated in associations or groups, facilitating the spread of such attacks. For this reason, analyzing the manifestations of this phenomenon should be considered, especially about authors' liabilities and modalities of conducts perpetrated[123].

The last views to take into consideration belongs to a member of academic institutions of the *Ad Hoc* Committee, the LUMSA University, Department of Law of Palermo. This delegation states that "cybercrimes can affect government functions, disrupting public telecommunications services and other critical infrastructures, and this is rarely limited to national borders. Reducing those risks is essential to ensure a stable, secure and peaceful cyberspace. Effective cooperation plays a pivotal role in order to collect a wide consensus creating a shared framework".

[123] See the Submission formulated by Centro Studi e Iniziative Culturali Pio La Torre, presented to the UNODC Secretariat, published in www.piolatorre.it

The LUMSA University deems that "the precise identification of norms and obligations will be instrumental in determining responsibility, bearing in mind that the breach of an obligation gives rise to international responsibility. It should be specified that the effectiveness of international cooperation cannot be limited only to the repression of those crimes structurally connected with the use of technology, but, it should be extended to offences of any kind committed through a computer system and also to those affected by the existence of digital evidence. In the context of the international judicial cooperation, dominated by the principle of territoriality and sovereignty, it is necessary to succeed in the difficult task of reconciling the needs underlying the organization of an effective activity of prevention, investigation and repression of cybercrimes with the rights of the individual"[124].

3.3 STATE OF PLAY AND FUTURE PERSPECTIVES OF THE *AD HOC* COMMITTEE

At present, the efforts of the *Ad Hoc* Committee have analyzed in detail some topics which constitute the core of the future UN Convention.

On criminalization, if on the one hand a uniform orientation is present about the inclusion of cyber-dependent crimes in a clear way and through a neutral technological language, adaptable to future ICTs or other techniques to commit crimes; on the other hand, several discussions are open about the inclusion of some cyber-enabled crimes, which will be clarified certainly in the next sessions.

As regard procedural measures and law enforcement, debates concerning specific procedural aspects were discussed, especially whether some disciplines should be regulated by domestic law or by the convention, for the purpose of admissibility of measures. Search, seizure and confiscation should be included in this new legal document as well as collection of information and data, preservation of stored data.

As it was said before, two orientations were counterposed about the structure of the new convention: Western countries like the United States of America, the United Kingdom and the European Union were in line with the path set by the Budapest Convention; the Russian Federation, China, Belarus and others expressed the will

[124] Based on the Submission formulated by LUMSA University, Department of Law of Palermo, submitted to UNODC Secretariat

to create a brand-new convention, with a specific focus on the fight against cybercrime.

In this moment, the orientation adopted by the *Ad Hoc* Committee seems to be a mediation between the inclusion of disciplines of existing instruments such as the Budapest Convention, UNTOC and UNCAC, and new rules, which analyze cybercrime in an innovative manner, thus without duplicate other legal documents. Moreover, the attention paid to multi-stakeholders guarantees a collaboration with Member States, allowing to give voice to individuals and organizations who suffer firsthand cyber-attacks: indeed, representatives of the third-sector are providing ideas, suggestions and proposals for the formulation of the new convention.

The next Third Session of the *Ad Hoc* Committee will be held in New York, from 29th August to 9th September 2022, and it will deal with provisions on international cooperation, technical assistance, preventive measures, mechanisms for implementation and final provisions.

The roadmap and mode of work adopted for the next meetings provide for interspersing of the *Ad Hoc* Committee sessions and the Intersessional Consultations dedicated to multi-stakeholders, to which the Chair and her team, together with the UNODC Secretariat, will submit consolidated negotiated documents, based on the outcomes of the first reading of the draft chapters of the convention. From the fourth session onwards, the Committee may consider the establishment of an open-ended group of experts with UN official languages skill that will be tasked, towards the end of the session, to ensure consistency of the whole text of the convention and in all official languages of the United Nations. In addition to that, a second reading of the topics already discussed will be made, soliciting inputs and suggestions to include in the convention together with some clarifications on the still open debates. The finalization and approval of the draft text of the convention is forecast for consideration and adoption by the General Assembly at its seventh-eighth session in 2024[125].

[125] "Proposed roadmap and mode of work of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" elaborated by the Chair of the *Ad Hoc* Committee

CONCLUSION

The use of information and communication technologies has changed society definitively, allowing a comprehensive connection with the world in real-time.
But it has led to a real escalation on criminality perpetrated in cyberspace: dynamic, anonymous and fleeing are the adjectives which can be certainly attributed to cybercrime. The latter is a very complex task, due to the multitude of entities involved, and their different means and methods.
In order to counter this criminal phenomenon, the convention currently under development is necessary to guarantee the harmonization of domestic legal systems and legislations on crime perpetrated through the use of ICTs.
Regional and international regulations already existent are insufficient as compared to the expanse of cybercrime, even if they are a significant starting point: indeed, these instruments provide for restricted collaborations, limited to Member States of some organizations or signatory ones. Whereas this transnational criminal conduct requires the intervention and the active participation of all States of the world, opting for joint operations, exchange of information and practices, and promoting capacity building, in order to increase the knowledge related to cyber-threats. This new convention in progress should long for a universal collaboration between States, institutions and organizations, including disciplines applicable also to future cybercrime's conducts, mechanisms on mutual legal assistance and training for judicial authorities to face this phenomenon.
The creation of the *Ad Hoc* Committee "to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" is useful not only to study and analyze cybercrime in detail, but mostly to ensure that the future convention is negotiated by Member States together with non-governmental organizations, civil society, private sector and academia, providing technical and specific competences.
This new legal document contemplates crime prevention and defense from the use of ICTs for criminal purposes, along with an effective and incisive response to it.
The study on which this thesis is based is the result of the writer's participation to the sessions of the *Ad Hoc* Committee to elaborate a new international convention on countering cybercrime. The attendance to the meetings has allowed a wide

comprehension about decision-making processes and formulation of international documents.

The mode of work adopted by the aforementioned *Ad Hoc* Committee guarantees participating Member States to express their proposals on the crime under consideration, making suggestions to include in the future convention, and describing their fieldwork, in reference to the incisiveness of cybercrime in single territories and, also the modalities adopted to counter it.

The discussions also concerned the choice of specific words, in order to avoid that future translations in the official UN languages could alter the meaning originally intended. Issues on interpretations could arise if terminology is not chosen accurately. Moreover, the use of some terms is recommended to maintain the same thread with other existing legal documents.

Member States, Observers and multi-stakeholders discuss on proposals elaborated by the Chair, providing new causes for reflection and new points of view on cybercrime. Everyone carries out certain needs and priorities that may not coincide with those of other subjects. For this reason, the real foundation of these sessions, and in general of the UN's work, is debate, considered as the main character of this scenario. At its core there is a common purpose to create a global convention which meets the needs of all. Debate is an inclusive and comprehensive method, without leaving anyone behind: States have the same importance, and contributions of anyone can make the difference. States, stakeholders and the UNODC team make common cause on an issue dangerous for everybody.

ADDENDUM

THE USE OF ICTS IN THE COVID-19 ERA

Information and communications technologies have allowed to face one of the biggest world crises of the current century, the Covid-19 pandemic.

The world was unprepared: nobody knew how to manage such a dramatic situation. Despite lockdowns and social distancing necessarily born brought to a great change of the balance of the society, ICTs have allowed to continue everyday life, creating new organizational set-up and routines such as distance learning, smart-working, online shopping. Students have had the possibility to keep going with their studies; workers have moved their activities on cyberspace, naturally according to the professions carried out. An important role has been played by social networks, and in general by digital platforms, which have allowed families to keep in touch.

These technologies have given a real contribution to societies, they have been the main characters during this pandemic, guaranteeing people to carry on, notwithstanding all different modalities of organization.

Even though several and remarkable positive effects have been made, there were likewise in the negative side, after a true abuse of information and communications technologies: studying through a computer could be exhausting, especially for children who keep attention scarcely. Staring a screen for hours, whether it belongs to a computer or to a smartphone, have caused not only physical problems, like postural ones or eye discomforts, but also psychological complications: people have isolated themselves, they have difficulties to socialize and express themselves, there is the fear to go out. ICTs represents a real comfort zone at this point.

In addition, discussions on Covid-19 and its vaccine generated a new way to spread disinformation and fake news, also through information and communications technologies, especially social networks. Even criminality has adapted to this new global situation.

Covid-19 pandemic have caused a great increase of cybercrime. Cybercriminals have taken advantages of this world crisis, weakening another “place”: cyberspace. These authors have acted mainly with phishing e-mails, misleading victims, sometimes buying online domains, or spreading DDos attacks and malwares like

ransomware. Cybercriminals' conducts can be considered looting: people, unprepared for the pandemic and the world crisis which derived, are also victims of this type of criminal behaviors, perpetrated by individuals who take advantages of this situation to make profits of every kind. Not by chance, the phenomenon of cyber-organized crime has increased strongly: whether it is stable organizations or temporary ones, the objective is to earn profit at the expenses of common people. Lockdowns forced by nations have convinced people to move the majority of their activities on the Internet, among which also banking transactions. Cybercriminals who manage telephonic or online fraud, pick on vulnerable individuals, such as elderly people, isolated ones, and children; the latter are often exposed to practices of online sexual exploitation, abuse and grooming, for instance with the OMEGLE platform. Also, cyber-espionage has spread a lot in the last few years, thus cyber-attacks that steal sensitive data to gain advantages over a competitive company or government entity.

And finally, one of the most perpetrated criminal conducts has been cyber-attacks and hacking to infrastructures, which caused the loss of a great amount of personal data and confidential information. Hospitals and health facilities has been the most targeted places during the pandemic, but together with the healthcare sector, energy and finance are the main objectives of the current authors of cybercrime[126].

An important purpose which governments want to achieve in the post Covid-19 era is the development of incisive protections against cybercrime, and to ensure a functional and efficient implementation of cybersecurity. Practices related to security in cyberspace are essential to protect sensitive data, infrastructure and in general the productive fabric. Investigative and judicial activities should be actualized in reference to the current problems of the society and in general of the world, guaranteeing sanctions proportionated to committed crimes. Governments should consider communicating and spreading as much information as possible on activities and methods related to cybercrime, in order to allow individuals to be careful and aware of cyber-attacks.

[126] P. MAHADEVAN, *Cybercrime: threats during the covid-19 pandemic*, Global Initiative against Transnational Organized Crime, 2020

CYBERSECURITY: A METHOD TO FACE CYBER-THREATS

In a world where life is become more and more social, or in general more digital, the risks to which people are exposed have increased considerably, in particular on the matter of financial losses, damage to the image of people and businesses, besides naturally loss of sensitive data and confidential information. For this reason, States of the world are developing new cybersecurity practices for countering as much as possible the increase of risks on the society.

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

The choice of the term "security" is not accidental; indeed, cybersecurity protects information from malicious software, threats, and in general cybercrime; it refers to data and information. Although commonly used as synonyms, "safety" has a different meaning indeed, it concerns how people can protect themselves from online threats; so, it refers to users.

Cybersecurity uses cryptographic protocols to encrypt e-mails, files and data, and safeguard them. Therefore, these methods are also used to protect against losses or thefts.

The main purpose of cybersecurity practices is to develop new defenses, identifying threats and elaborating new modalities to combat them[127].

It is based on three fundamental principles (so-called CIA Triad): confidentiality which wants to guarantee that data and resources are preserved from the possible use or access by unauthorized people. This principle should be ensured since the storing of information. Integrity means the ability to keep veracity of data and information, guaranteeing they will not be modified or canceled by unauthorized individuals. And the last principle is availability which corresponds to the possibility to authorized people to access to resources whenever they want[128].

[127] L. PICOTTI, *Cybersecurity: quid novi?*, Dir. Internet, 2020
[128] W. CHAI, *Confidentiality, Integrity and Availability (CIA Triad)*, www.techtarget.com, 2021

Cybersecurity should guarantee that a service or data are preserved by these three principles. If one of them is violated, the system is exposed to vulnerabilities and probably an attack to services or data is in progress. Its practices are applied to many contexts, from business to mobile computing.

In detail, web security consists in the defense of information technology webs from fraudulent actions, such as targeted attacks or opportunistic malware.

Another type of security concerns applications, with the aim to protect software and devices from eventual threats. A compromised application could allow the access to data, which should be protected.

Integrity and privacy of data, both stored ones and temporary ones, are protected by the so-called information security, whereas operating security includes processes and decisions on managing and protection of data assets. It includes authorizations used by users to access to web, and procedures which determine how and when data could be stored or shared.

Therefore, disaster recovery and business continuity are strategies used by businesses to respond to cybersecurity accidents, and in general those events which provoke a loss of operations or data. Policies of disaster recovery indicate procedures useable to refresh operations and businesses' information, in such a way to go back to the same operating capacity there was before the accident. Business continuity is the plan adopted by enterprises for operating without certain resources. Everyone who does not respect security procedures risks accidentally to insert a virus in a system originally safe[129].

Indeed, cybersecurity can be threatened in different ways: as it was already said, the spread of malware is the most common operation conducted by cybercriminals, who use for example viruses, programs capable of self-replicating, which infect clean files. Another malware attack perpetrated is through trojan, a malware concealed behind a legitimate software. Cybercriminals persuade users to download trojan in their computers, and then cause damage or collect data[130]. Spyware is a program which secretly register actions of uses, allowing cybercriminals to take advantages from information. For instance, spyware collect credit card data. As it

[129] See *What is cybersecurity*, www.kaspersky.com
[130] See www.mcafee.com

was said, another type of malware used is ransomware, which block the access to users' data and files, threatening to cancel them if victims do not pay a ransom. Adware is an advertising software which can be used to spread malware. Botnet is composed of a series of computer infected by malware, used by cybercriminals to overload websites with requests to access.

Together with the spread of these types of malware, there are also other conducts which can be perpetrated in order to damage cybersecurity, for instance insert of a structured language query code, the so-called form-jacking. It is a type of cyber-attack with the aim to take control of a database and stole data. Cybercriminals take advantages from vulnerabilities of data-driven applications to insert a malicious code in a database through damaging SQL instructions, which allow them to access to sensitive information stored in the database.

Other common cyber-threats include backdoors which allow remote access, phishing and denial-of-service attacks (DDoS).

Generally, these practices belong to a unique category called social engineering: specific cyber-attacks based on the study of people's conducts, in order to manipulate them and swipe confidential information. To bring about these types of assaults, cybercriminals study victims' behaviors and movements accurately; if the target is a business, information about employees are collected. Social engineering is perpetrated mainly through e-mails, websites or phone-calls.

Teaching users to cancel suspicious e-mail attachments and adopt some important precautions is essential for the security of every business. Formation of final users is one of the most important aspects of cybersecurity, because generally these individuals are the immediate victims of such attacks. Cybercriminals exploit vulnerabilities of people, who probably do not have information technology competences.

Indeed, various practices could be brought about by both users and businesses to protect from criminal attacks: first of all, updating software and operating systems because the upgrade enhance IT security of devices, putting under cover from hacker attacks, and it also allows to obtain new functions and improve performances.

Using an antivirus software is appropriate to identify threats, conducting periodical scans so verifying the eventual presence of suspicious elements in the device.
Another method used a lot is the so-called cloud security, protecting data and information within the aforementioned clouds, running backups for the duplication of files, photos, conversations and in general contents belonging to the instrument.
Avoiding opening e-mail attachments or links from unknown senders is also a common practice, because they may contain infected malware.
A common practice is the credentials update as well as the use of complex passwords, hard to guess. Fortunately, nowadays almost all the websites that foresee the registrations suggest to use long words with specific characters such as numbers, special keyboard characters.
One of the most discussed matters of the last few years is the use of the Artificial Intelligence. Indeed, AI allows to strengthen and enhance predictive skills of systems in defense of businesses and organizations, making realistic previsions on attacks and risks. It handles not only with the identification of threats and investigations on online activities conducted, but it acts also through prevention, protecting sensitive data contained in devices.
Artificial Intelligence stores habits and modalities which users have when they operate on the Internet. An anomalous conduct is immediately noticed and monitored, and when needed this action is stopped[131].
Cybersecurity should be implemented both at national and international levels. Security of single countries is functional to protect digital environment, but it is not enough if the borderless nature of cyberspace is taken into account, where a threat is global potentially. For this reason, to reach an efficient and effective cybersecurity is necessary coordination among defense and legal systems, technical capacities together with local and global institutions.

[131] EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Artificial Intelligence Cybersecurity Challenges*, 2020

THE CONSEQUENCES OF THE RUSSIAN-UKRAINIAN WAR ON THE WORK OF THE *AD HOC* COMMITTEE

During the First and the Second Sessions of the *Ad Hoc* Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, a lot of distinguished delegates of Member States and also representatives of stakeholders expressed their full solidarity with Ukraine, strongly condemning the attack perpetrated by the Russian Federation.

As it was said in this thesis, the Russian Federation promoted actively the elaboration of a new United Nations Convention on cybercrime. But, in this historical time period, this State is no longer in the position of credibility and reliability which it may have before; the interventions proposed during the meetings of the sessions were not much considered by Member States, indeed some of them even proposed an ousting of the negotiation, for the violation of the United Nations Charter and of the international humanitarian law.

To that, the Russian Federation responded exhorting Member States to focus on the work of the *Ad Hoc* Committee related to cybercrime, without any kind of interference with the international political situation. Certainly, tensions run high: this palpable discontent does not aid the negotiation activity for the formulation of the new convention, with the resulting deterioration of the international framework.

The war in Ukraine is not only a physical conflict: it involves also cyberspace, through cyber-assaults against infrastructures and hacker attacks to the respective Russian and Ukrainian governments, but also to other countries, and controls on the spread of information. On the one hand, the Russian Federation tries to censure news, banning the use of social media and disseminating fake news; on the other hand, multinational groups such as Netflix, Google, Apple, Amazon and others are cutting services, suspending or ending their activities in the Russian territory. Even Anonymous, the famous organization of hacktivists (hacker and cyber-activists) declared telematic war to the Russian Federation, assaulting state websites and transmitting TV messages against the President Vladimir Putin. In the meantime, the North Atlantic Treaty Organization (NATO) is developing new defensive

techniques on cybercrime, also in reference to Russian cyber-operation of aggression to data and infrastructures. Indeed, thanks to the NATO Cooperative Cyber Defense Center of Excellence, the Tallinn Manual 2.0 was elaborated, a guide for politicians and experts on how international law can be applied on IT operations among and against States.

At this point, it can be said with certainty that wars, at the time of 2022, have as scenarios also cyberspace, which becomes a true battle field, more and more present, especially with cyber-attacks to infrastructures and governments, able to cause a strong impact on the society and international relations[132].

[132] I. TENNANT, S. WALKER, *Cyber, fire and fury*, Global Initiative against Transnational Organized Crime, Vienna, 2022

REPRESENTATIVES OF GLOBAL AND REGIONAL INTERGOVERNMENTAL ORGANIZATIONS, INCLUDING REPRESENTATIVES OF UNITED NATIONS BODIES, SPECIALIZED AGENCIES AND FUNDS, AS WELL AS REPRESENTATIVES OF FUNCTIONAL COMMISSIONS OF THE ECONOMIC AND SOCIAL COUNCIL

- COUNCIL OF EUROPE
- EUROPEAN PUBLIC LAW ORGANIZATION
- EUROPEAN UNION INSTITUTE FOR SECURITY STUDIES
- INTERNATIONAL CENTRE FOR CRIMINAL LAW REFORM AND CRIMINAL JUSTICE POLICY
- INTERNATIONAL CHAMBER OF COMMERCE
- INTER-PARLIAMENTARY UNION
- INTERNATIONAL CRIMINAL POLICE ORGANIZATION - INTERPOL
- KOREAN INSTITUTE OF CRIMINOLOGY AND JUSTICE
- ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
- ORGANIZATION OF AMERICAN STATES
- ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE
- THE COMMONWEALTH SECRETARIAT
- THE WORLD BANK
- UNITED NATIONS CHILDREN'S FUND
- UNIVERSITY FOR PEACE

REPRESENTATIVES OF NON-GOVERNMENTAL ORGANIZATIONS THAT ARE IN CONSULTATIVE STATUS WITH THE ECONOMIC AND SOCIAL COUNCIL, IN ACCORDANCE WITH COUNCIL

- ACCESS NOW
- AFRICA ALLIANCE FOR HEALTH, RESEARCH AND ECONOMIC DEVELOPMENT
- AFRIQUE ESPERANCE
- APOSTLE PADI OLOGO TRADITIONAL BIRTH CENTRE

- APPUI SOLIDAIRE POUR LE RENFORCEMENT DE L'AIDE AU DEVELOPPEMENT
- ARTICLE 19 – INTERNATIONAL CENTRE AGAINST CENSORSHIP
- ASABA HOME-DIASPORA
- DEVELOPMENT INITIATIVE ASSOCIATION ADALA JUSTICE
- ASSOCIATION FOR COMMUNITY AWARENESS (ASCOA)
- ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS
- ASSOCIATION POUR L'INTÉGRATION ET LE DÉVELOPPEMENT DURABLE AU BURUNDI
- BUREAU POUR LA CROISSANCE INTÉGRALE ET LA DIGNITÉ DE L'ENFANT
- CENTER FOR THE STUDY OF CRIME
- CENTRO INTERNAZIONALE SINDACALE PER LA COOPERAZIONE SVILUPPO
- CENTRO STUDI ED INIZIATIVE CULTURALI PIO LA TORRE
- CLUB OHADA THIES
- CONCERN FOR HUMAN WELFARE
- CRIMINOLOGISTS WITHOUT BORDERS
- CYBER CAFÉ AVENIR POUR TOUS
- CYBER INSTITUTE
- DEVELOPMENT GENERATION AFRICA INTERNATIONAL (DGAI)
- EARTH PUSH LTD/GTE
- ELIZKA RELIEF FOUNDATION
- END CHILD PROSTITUTION, CHILD PORNOGRAPHY AND TRAFFICKING OF CHILDREN FOR SEXUAL PURPOSES. INC.
- FESTHES "FESTIVAL POUR LA SANTÉ»
- FIRST MODERN AGRO. TOOLS COMMON INITIATIVE GROUP (FI.MO.AT.C.I.G)
- FOUNDATION FOR HUMAN HORIZON
- GLOBAL DEAF MUSLIM FEDERATION
- GREEN AND BETTER WORLD

- HAMRAAH FOUNDATION
- HAWAU ENIOLA FOUNDATION
- HEAVENLY SHOWER OF PEACE CHURCH OF GOD
- HUMAN RIGHTS SANRAKSHAN
- SANSTHAA
- HUMAN RIGHTS WATCH
- IDPC CONSORTIUM
- ICT FOR PEACE FOUNDATION
- IJEOMA FOUNDATION FOR THE OLD PEOPLE
- INSTITUT MOBILE D'EDUCATION DÉMOCRATIQUE (IMED)
- ISTITUTO IGARAPÉ
- INTERNATIONAL ASSOCIATION OF PENAL LAW
- INTERNATIONAL FUND FOR ANIMAL WELFARE
- INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
- INTERNET SOCIETY
- LEBANESE CYBERSPACE ASSOCIATION
- MAAT FOR PEACE, DEVELOPMENT AND HUMAN RIGHTS
- MEDIA FOUNDATION FOR WE AFRICA
- MORE TRUST
- NATIONAL COUNCIL OF CHILD RIGHTS ADVOCATES, NIGERIA: SOUTH WEST ZONE
- NOBILE INSTITUTION FOR ENVIRONMENTAL PEACE INC.
- OHAHA FAMILY FOUNDATION
- ORGANISATION INTERNATIONALE POUR LE DÉVELOPPEMENT ÉCONOMIQUE SOCIAL AND HUMANITAIRE
- O.N.G. DERECHOS DIGITALES
- PEACEEVER TV INTERNATIONAL MEDIA GROUP INC.
- POMPIERS HUMANITAIRES
- PRIVACY INTERNATIONAL
- RED DOT FOUNDATION
- RESEAUX I.P EUROPEENS NETWORK COORDINATION CENTRE

- "SEG" CIVIL SOCIETY SUPPORT CENTER NGO
- SANID ORGANIZATION FOR RELIEF AND DEVELOPMENT
- SIFTUNG WISSENSCHAFT UND POLITIK
- SILVER LINING FOR THE NEEDY INITIATIVE
- SIRACUSA INTERNATIONAL INSTITUTE FOR CRIMINAL JUSTICE AND HUMAN RIGHTS
- SOCIETY FOR THE WIDOWS AND ORPHANS
- STIFTUNG WISSENSCHAFT UND POLITIK
- THE CENTER FOR OCEANIC AWARENESS, RESEARCH AND EDUCATION
- TRANSPARENCY INTERNATIONAL
- WILDLIFE CONSERVATION SOCIETY
- YERIMA BALLA INTERNATIONAL EDUCATION LIMITED
- YOUNG PROFESSIONAL DEVELOPMENT SOCIETY NEPAL
- ZONTA INTERNATIONAL

REPRESENTATIVES OF OTHER RELEVANT NON-GOVERNMENTAL ORGANIZATIONS, CIVIL SOCIETY ORGANIZATIONS, ACADEMIC INSTITUTIONS AND THE PRIVATE SECTOR

NON-GOVERNMENTAL ORGANIZATIONS

- ACTION POUR LES DROITS HUMAINS AU NIGER
- ALLIANCE OF NGOS ON CRIME PREVENTION AND CRIMINAL JUSTICE
- ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA
- CROSS-BORDER DATA FORUM
- CYBERPEACE INSTITUTE
- CYBERSECURITY COALITION
- CYBERSECURITY TECH ACCORD
- FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS, INC.
- HUMANITY FOR THE WORLD
- LEGAL ANALYSIS AND RESEARCH PUBLIC UNION/HÜQUQI TƏHLIL VƏ ARAŞDIRMALAR İCTIMAI BIRLIYI

- OBSERVER RESEARCH FOUNDATION AMERICA
- OPEN DREAMS ORGANIZATION INC.
- RAPHA HOUSE INTERNATIONAL
- RED EN DEFENSA DE LOS DERECHOS DIGITALES
- STICHTING GLOBAL FORUM ON CYBER EXPERTISE
- UNITED NATIONS DIPLOMATIC COMMITTEE INTERNATIONAL ORGANIZATION

CIVIL SOCIETY

- ACTION CITOYENNE POUR L'INFORMATION ET L'ÉDUCATION AU DÉVELOPPEMENT DURABLE (ACIEDD)
- ANTI-PHISHING WORKING GROUP
- ASOCIATIA ELIBERARE
- ASSOCIATION AIDE AUX FEMMES ET ENFANTS
- ASSOCIATION DES NATIONS UNIES POUR LE TCHAD
- CENTER FOR COOPERATION IN CYBERSPACE
- CENTER FOR DEMOCRACY AND RULE OF LAW
- CENTER FOR DEMOCRACY AND TECHNOLOGY
- CHILDREN AND YOUNG PEOPLE LIVING FOR PEACE (CYPLP)
- CYBERSECURITY PLATFORM OF THE AUSTRIAN GOVERNMENT
- DEUTSCHER EDV-GERICHTSTAG E.V.
- ELECTRONIC FRONTIER
- FOUNDATION
- FOUNDATION FOR INTERNATIONAL BLOCKCHAIN AND REAL ESTATE EXPERTISE
- GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME
- GLOBAL PARTNERS DIGITAL LIMITED
- INTERNATIONAL POLICE SCIENCE ASSOCIATION (IPSA)
- JONCTION
- JUDGE STEIN SCHJOLBERG

- STIFTUNG NEUE VERANTWORTUNG E.V.
- STIMSON CENTER

ACADEMIC INSTITUTIONS

- BEIHANG UNIVERSITY
- BOURNEMOUTH UNIVERSITY
- CYBERLAW UNIVERSITY
- INSTITUTE FOR PEACE RESEARCH AND SECURITY POLICY AT THE UNIVERSITY OF HAMBURG (IFSH)
- JOHN JAY COLLEGE OF CRIMINAL JUSTICE
- KOREAN NATIONAL POLICE UNIVERSITY
- LUMSA UNIVERSITÀ – DIPARTIMENTO DI GIURISPRUDENZA (PALERMO)
- SAARBRÜCKER ZENTRUM FÜR RECHT UND DIGITALISIERUNG
- STRATHMORE UNIVERSITY
- TEMPLE UNIVERSITY JAMES E. BEASLEY SCHOOL OF LAW, INSTITUTE FOR LAW, INNOVATION & TECHNOLOGY
- UNIVERSITY OF ADELAIDE
- UNIVERSITY OF HUDDERSFIELD
- UNIVERSITY OF LAUSANNE
- UNIVERSITY OF LODZ
- UNIVERSITY OF PENNSYLVANIA
- UNIVERSITY OF WEST ATTICA
- XIAMEN UNIVERSITY SCHOOL OF LAW

PRIVATE SECTOR

- AMAZON WEB SERVICES
- BI.ZONE
- CHAMBER OF COMMERCE OF THE USA
- DB CONNECT
- DELOITTE RISK ADVISORY BV
- IMR & ASOCIADOS SRL

- KASPERSKY
- MANDIANT
- META
- MICROSOFT
- MODERN WEB IDEAS
- NCC GROUP
- N-GATE LTD.
- PRIVANOVA
- SAEM CORPORATION
- THE NETWORK EXORCIST