7TH INTERNATIONAL ZEUGMA CONFERENCE ON SCIENTIFIC RESEARCHES

January 21-23, 2022

Gaziantep, Turkey

THE BOOK OF FULL PAPERS

VOLUME 1

Editor: Dr. Mahir KOTUK

THE BOOK OF FULL PAPERS

Editor:
Dr. Mahir KOTUK

by
IKSAD GLOBAL PUBLISHING HOUSE®

Issued: 09.02.2022

ISBN - 978-625-7464-72-7

CYBERCRIME AND THE COUNCIL OF EUROPE BUDAPEST CONVENTION: PREVENTION, CRIMINALIZATION, AND INTERNATIONAL COOPERATION

Prof. Dr. Ana CAMPINA (PhD)[1*],
[1] Universidade Fernando Pessoa; Instituto Jurídico Portucalense, Porto, Portugal.
ORCID ID: 0000-0003-0820-1280

Prof. Dr. Carlos RODRIGUES (PhD)[2]**
[2] Universidade Fernando Pessoa; Instituto Jurídico Portucalense, Porto, Portugal.
ORCID ID: 0000-0003-0966-6274

Abstract

The Budapest Convention on Cybercrime (2001) and their Additional Protocols (2021) is considered as one coherent international agreement and the base to prevent, combat and criminalize this dangerous crime. The International Law and the national legislations are being developed according to this Convention, based on the strategic (re)action to this crime that is increasing with the worst consequences all around the world.

The Rule of Law were obliged to develop their legislation, mainly Penal Law, considering the emergent need to answer to the most serious violations of the fundamental and the Human rights of their citizens, using the most modern technology through the internet, with capacity and efficacy that seriously affect all dimensions of life.

The Budapest Convention on Cybercrime provides the criminalization of conduct; the procedural powers to the criminal investigation; and the International Cooperation as one of the most efficient and law enforcement to prevent and combat the Cybercrime. The 77 States Participants close working with the States Observers, within the International Cooperation strategy, connected with Governments, police authorities (national and international), International Organizations and Institutions have been the more profitable strategic (re)action, promoting the cooperation position to the emerging challenges, although the cybercrime is one of the hardest crimes to face. So, there is an evolution in the instruments and strategies to prevent and combat the Cybercrime, but there is an urgent need of an effective legal and social (re)solution, otherwise there will have world and human irreversible impacts.

Finally, from the law and cybercrime challenges, the strategy is largely confirmed by the cooperation: the sharing a) information within the legal frameworks; b) the response – operational or tactical; c) the works in the Darkweb; the market, financial and economic movements facing the cybercrime or to denounce the cybercriminals; d) transparency to prevent the cybercrime evolution and implementation.

Keywords: International Cooperation; Cybercrime; Council of Europe; International Law; Criminalization

INTRODUCTION

Since last decades, the virtual life that Humanity and the States have been facing a permanent and a dangerous threat, the cybercrime. The globalization, the technologic and the computer systems evolution, as well as the internet vulgarization and dependence by the biggest part of the individuals, institutions, and States, have cause opportunities to implement this crime that is affecting all virtual life dimensions.

The cybercrime worldwide evolution has been quicker than the political and legal position and reaction to prevent and to combat it but, in fact, it´s undoubtable that there has been a significant development of the political and legal – juridical and judicial – reply and recognizing this crime. The International Community is aware and reacting to avoid the most serious consequences of the cybercrime, but the Council of Europe in last two decades, after the Budapest Convention on Cybercrime (2001), assumed the international leadership of the prevention and combat it, providing the criminalization of conduct;

the procedural powers to the criminal investigation; and the International Cooperation as one of the most efficient and law enforcement to prevent and combat the Cybercrime.

As a problem to everyone and to all world structures, this research allows us to collect elementary legal and update data information to achieve different worried conclusions of the dimension of cybercrime problem – human, political, economic, financial, cultural – which impacts affects seriously the International, States and individual security. It´s confirmed that International Cooperation is one of the most important strategies that the Council of Europe is promoting and request to face this criminality. This important International Organization by legal instruments, structures and programs focusing on the Cybercrime problem has been crucial to their States Members but as a worldwide spread.

As a study case, this paper presents the research and the conclusions of the cybercrime and the legal reaction of Portugal, mainly in the legal context. In the same line of the international tradition, it has created a set of legal assets essential to the organization of society that are under the purview of criminal law, national legislation enshrines in the criminal system a set of computer offenses covered by that criminal law.

Finally, we present an analysis and an interpretation of the Council of Europe Budapest Convention on Cybercrime, as well the Additional Protocols and other legal instruments and structures, as fundamental mechanisms to prevent and effectively combat the Cybercrime worldwide.

The conclusions are so important as worrying for the International Security and the difficulties of the authorities to control the cybercriminal, which consequences are affecting or would affect everyone and structures worldwide. This is one of the most serious challenges of the actuality.

MATERIALS

According to Steve Morgan (Nov. 13, 2020) [1], in the "*Special Report: Cyberwarfare in the C-Suite*", if a global assessment of cybercrime were carried out, "*which is predicted to inflict damages totaling $6 trillion USD globally in 2021 – would be the world's third-largest economy after the U.S. and China*".

This means, according to the same author, that the "*Global Cybercrime Damage Costs*" would be *"$6 trillion USD a year, $500 billion a month, $500 billion a week, $16,4 billion a day, $684,9 million an hour, $11,4 million a minute and $190,00 a second*".

Also, according to the same author, (Steve Morgan, Nov. 13, 2020), "*the 2017 report from Cybersecurity Ventures predicted ransomware damages would cost the world $5 billion in 2017, up from $325 million in 2015 — a 15x increase in just two years. The damages for 2018 were estimated at $8 billion, and for 2019 the figure rose to $11.5 billion*".

The use of the computer as a tool for work and leisure, leads that author to Steve Morgan (Nov. 13, 2020) predict that "*by 2023, there will be 3x more networked devices on Earth than humans, according to a report from Cisco. And by 2022, 1 trillion networked sensors will be embedded in the world around us, with up to 45 trillion in 20 years*", and that, in view of the consequent internet connection, it is foreseen that "*IP traffic has reached an annual run rate of 2.3 zettabytes in 2020, up from an annual run rate of 870.3 exabytes in 2015*".

The world population is so dependent on the Internet that, according to the ITU – International Telecommunication Union in 2019, "*More than 50% of the world's population is now online"*[2]. In addition to this already large number of internet users, there is a significant increase in new internet

[1] Steve Morgan, Editor-in-Chief, in Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybercrime Magazine, Sausalito, Calif. (Nov. 13, 2020) https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, consulted in 2022-01-27.

[2] ITU (International Telecommunication Union). (2019). Measuring Digital Development: Facts and Figures 2019. Geneva: ITU. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf , consulted in 2022-01-27.

users every day, since according to Kemp, S., 2019, *"roughly one million more people join the internet each day*".[3]

Evidently, these new means of communication and interconnection of people, companies, International Organizations and States, attract the criminal world to use it in their criminal activities. Indeed, cyber-attacks have become a constant danger for all Internet users, a fact that is highlighted by the *The Global Risks Report 2020* (15th Edition), of the World Economic Forum, p. 62), when stating that "*cyberattacks have become a common hazard for individuals and businesses: our surveys rank them as the seventh most likely and eighth most impactful risk, and the second most concerning risk for doing business globally over the next 10 years*."[4] According to the same report by the World Economic Forum, the "*cyberattacks on critical infrastructure — rated the fifth top risk in 2020 by our expert network — have become the new normal across sectors such as energy, healthcare, and transportation. Such attacks have even affected entire cities*". This report by the World Economic Forum refers those cybercriminals are sure that there is great difficulty in being detected and incriminated, in fact, as it is stated there that the "*Organized cybercrime entities are joining forces, 13 and their likelihood of detection and prosecution is estimated to be as low as 0.05% in the United States*."

METHODS

Along the research and the writing of this paper we applied mainly a qualitative methodology but with strategic and fundamental statistic data, as a key for the study object analysis and the scientific conclusions and paper production.

The research conducted us to the legal and the political analysis, in a worldwide cybercrime study, but focus on the International Law – mainly the Council of Europe and the Budapest Convention on Cybercrime, as well as the "Portugal and the Cybercrime" study case. This research studied data/ information and studies as updated as available, supported in scientific information to explain the Cybercrime and the Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation.

RESULTS

The consequence of this intense worldwide activity through the Internet has led to its use for the practice of criminal activities, either for the continuation of the practice of old criminal systems, or for the practice of new types of crime.

According with the FBI/IC3 – Federal Bureau of Investigation/ Internet Crime Complaint Center, in his report "*Internet Crime Report-2020, pp. 3*"[5], IC3 received a record number of complaints from the American public in 2020: 791,790, stating that "*with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019. Business E-mail Compromise (BEC) schemes continued to be the costliest: 19,369 complaints with an adjusted loss of approximately $1.8 billion. Phishing scams were also prominent: 241,342 complaints, with adjusted losses of over $54 million. The number of ransomware incidents also continues to rise, with 2,474 incidents reported in 2020.*"

It´s clear in this "*Internet Crime Report – 2020*" how the cybercrime activity, only in United States has caused extremely high damage to that State's economy.

In the same report – *FBI/IC3 – Federal Bureau of Investigation/ Internet Crime Complaint Center* there is a chart (p. 6) showing the evolution of the criminality within their criminal activities of "phishing / vishing / smishing / pharming", "non-payment / non-deliver", "extortion", "personal data breach" and

[3] Kemp, S. (2019). "Digital 2019: Global Digital Overview". Datareportal. https://datareportal.com/reports/digital-2019-global-digital-overview , consulted in 2022-01-27.

[4] The Global Risks Report 2020 - 15th Edition, of the World Economic Forum In partnership with Marsh & McLennan and Zurich Insurance Group - https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf - consulted in 2022-01-27.

[5] Internet Crime Report-2020, FBI/IC3 – Federal Bureau of Investigation/ Internet Crime Complaint Center - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf - consulted in 2022-01-27.

"identity theft", where it´s possible to state the growing activity between the years, from 2016 to 2020, as following: (Figure 1).[6]

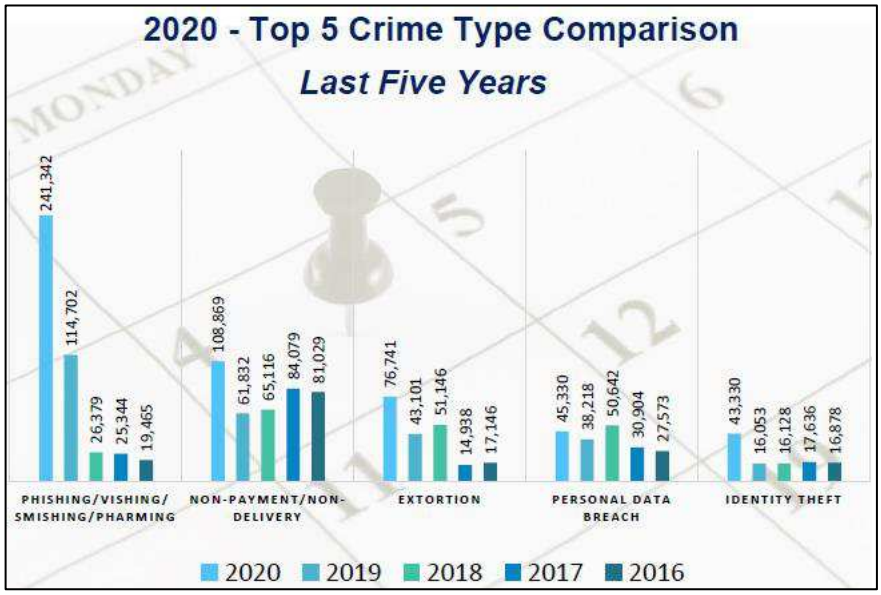

Figure 1 – 2020 – Top 5 Crime Type Comparison Last Five Years

The same United States internal security organization shows us in that report that this intense criminal activity through computerized means caused in those years, from 2016 to 2020, a growing increase in investigation processes and a high monetary loss for victims of cybercrime, incidentally visible on (Figure 2)[7], as following:

Figure 2 – 2020 – Total Complaints and Total Losses

[6] *Idem.*

[7] Internet Crime Report-2020, FBI/IC3 – Federal Bureau of Investigation/ Internet Crime Complaint Center - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf - consulted in 2022-01-27.

The same report of FBI/IC3 – Federal Bureau of Investigation/ Internet Crime Complaint Center, p. 17, that United States security force presents the States worldwide that were more affected by this criminal activity, as we present in following figure (Figure 3)[8].

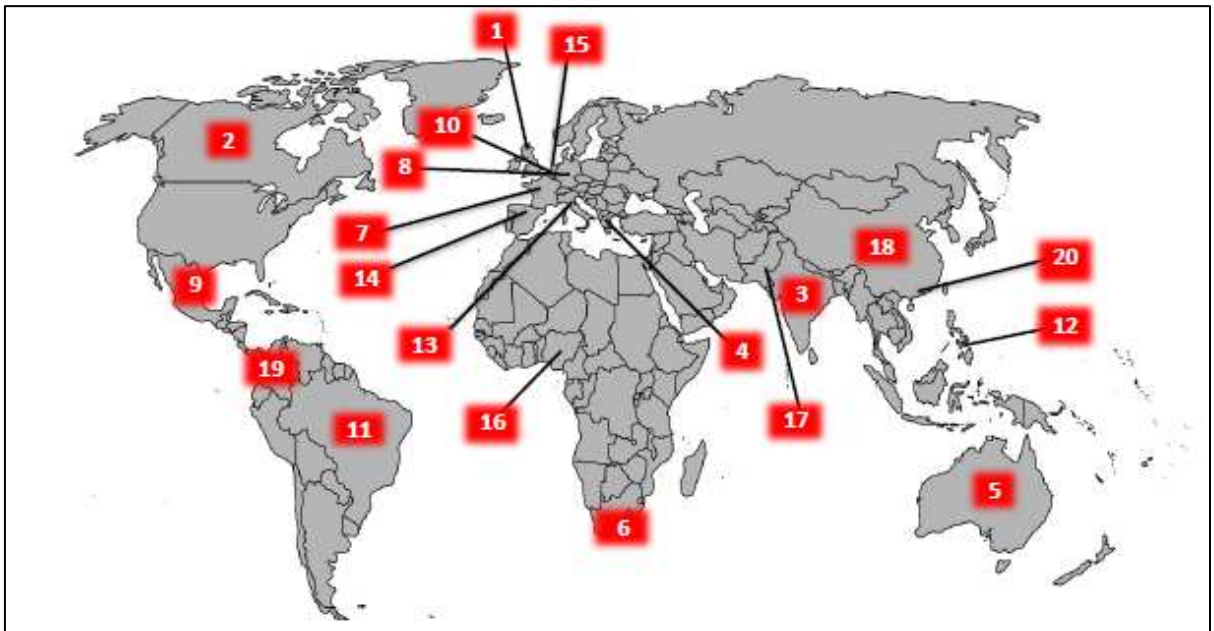

Figure 3 – 2020 – Top 20 International Victim Countries – Excluding the United States of America

Concerning the vulnerability of companies and organizations, we found that worldwide all of them can be attacked by cybercriminals, as we have identified with the data extracted from the website of "STATISTA" as we present bellow as a Table (Table 1)[9] where is evident that regardless of the size of the company and the branch of its activity, all can be attacked by cybercrime.

Characteristic	Total	Small	Large	Unknown
Total	29,207	1,037	819	27,351
Accommodation	69	4	7	58

[8] Internet Crime Report-2020, FBI/IC3 – Federal Bureau of Investigation/ Internet Crime Complaint Center - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf - consulted in 2022-01-27.

[9] *in* Statista 2022 - Data breaches worldwide 2020, by victim industry and size - Published by Joseph Johnson - Jun 4, 2021 - https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/ consulted in 2022-01-27.

Characteristic	Total	Small	Large	Unknown
Administrative	353	8	10	335
Agriculture	31	1	0	30
Construction	57	3	3	51
Education	1,332	22	19	1,291
Entertainment	7,065	6	1	7,058
Finance	721	32	34	655
Healthcare	655	45	31	579
Information	2,935	44	27	2,864
Management	8	0	0	8
Manufacturing	585	20	35	530
Mining	498	3	5	490
Other Services	194	3	2	189
Professional	1,892	793	516	583
Public	3,236	22	65	3,149
Real Estate	100	5	3	92
Retail	725	12	27	686
Trade	80	4	10	66
Transportation	212	4	17	191
Utilities	48	1	2	45
Unknown	8,411	5	5	8,401

Table 1 – Global number of cyber security incidents in 2020, sorted by victim industry and organization size

DISCUSSION

It´s relevant to understand that the data that we have exposed shows the dependence generated by the exponentially growing use of the Internet, and the new means that computers technology have made available to humanity, bring with them a new type of criminality, or its use by the old criminality but now adapted with the use of these computing and connection and interconnection, so, meaning that the entire world population has come to use.

The discussion that we will present to the readers of this paper translates into the legislation that countries had to create to prevent and combat cybercrime, either internally or in cooperation within different States, and in what to bring to the discussion at an international level. So, we will make a brief analysis of the Budapest Convention on Cybercrime and the Council of European (re)action.

1. Portugal and the Cybercrime

In fact, by all that the Rules of Law are essentially concerned with ensuring that criminal proceedings protect the fundamental rights of society to guarantee the existence of social peace, in a constant search for balance on the guarantee of fundamental individual rights and the need to defend society and personal and community legal interests.

Following the international tradition, Portugal, therefore created a set of legal assets essential to the organization of society that, are under the scope of criminal law, and, specifically for what we now and here analyze, the national legislation enshrines in the penal system a set of computer offenses covered by that criminal law.

We will do, therefore, and in what we present here, an analysis of the computer crimes provided for in the Cybercrime Law.

The computer crime conceptualization was worked on 2006 by the authors Garcia Marques and Lourenço Martins, in their publication *Direito da Informática*, page 639, presenting the conceptualizing and the definition of computer crime as "…*any act in which the computer serves as a means to achieve a criminal purpose or where the computer is the symbolic target of that act or where the computer is the object of crime*." (Marques & Martins, 2006, p. 639)[10]

The computer crimes essential typology is dispersed by the Budapest Convention, which will be analyzed in the following item, while here we will present a brief analysis of the Cybercrime Law provided for in Portuguese Law n. 109/2009, of 15 September[11], with the changes introduced by Law n. 79/2021, of 24 November.[12]

Following, let's focus on to this descriptive analysis.

The "*Crime of computer falsehood*", recognized by Article 3 of the Cybercrime Law, has the legal interest of protecting the "*integrity of information systems*", thus being a crime of result, "...*through which it is intended to prevent acts committed against the confidentiality, integrity and availability of*

[10] Marques, G. & Martins, L. – 2006 – Direito da Informática (2.ª Refundida). Coimbra: Almedina – Portugal, p. 6.

[11] The consultation of the Law n. 109/2009, September 15th, can be done on the website CoProcuradoria-Geral Distrital de Lisboa do Ministério Público in the link - https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis – consulted in 2022-01-27.

[12] The consultation of the Law n. 79/2021, November 24th, can be done on the website CoProcuradoria-Geral Distrital de Lisboa do Ministério Público in the link - https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3476&tabela=leis&ficha=1&pagina=1&so_miolo= – consulted in 2022-01-27.

computer systems, networks and computer data as well as the fraudulent use of these computer systems, networks and data…" as said Pedro Dias Venâncio. (Venâncio, 2021, p. 85)[13]

The "*Crime of damage related to programs or other computer data*", recognized by Article 4 of the Cybercrime Law, has the legal interest to protect *"…the integrity of computer systems and, indirectly, the digital heritage of the victim…*", thus being a dangerous crime, *"…as these acts are penalized regardless of whether there is damage or not*". (Venâncio, 2021, pp. 83-84)[14]

The "*Crime of computer sabotage*", recognized by Article 5 of the Cybercrime Law, has the legal interest to protect *"…the normal circulation of information and its value as an operational unit that allows fluid communication and data storage…*" (Venâncio, 2021, p. 87) [15] being, this way, a crime of result.

The "*Crime of illegitimate access*", recognized by Article 6 of the Cybercrime Law, has the legal interest to protect *"…the security of the computer system, that is, the protection of the so-called "computer domicile", something similar to the introduction in someone else's house..."*, being here evident that we are dealing with a crime of danger because the law does not specifically require the agent to commit any damage or benefit from the practice of the crime. (Venâncio, 2021, pp. 81-82)[16]

The "*Crime of illegitimate interception*", recognized by Article 7 of the Cybercrime Law, has the legal interest of protecting *"…the security and privacy of electronic communications…*" (Venâncio, 2021, p. 88) being a crime of result, as well.[17]

The "*Crime of illegitimate reproduction of a protected program*", recognized by paragraph 1 of Article 8 of the Cybercrime Law, has the legal right to protect *"…the copyright on the computer program and the protection of intellectual property as an element of economic development…*" (Venâncio, 2021, p. 89)[18], being a crime of result, too.

The "*Crime of illegitimate reproduction of topographies and semiconductor products*", recognized by paragraph 2 of Article 8 of the Cybercrime Law, has the legal interest of protecting the copyright on the topography of a semiconductor product. There are those who understand that this crime is the same as the crimes provided for in Articles 318 and 321 of the Industrial Property Code, so it would be totally "consumed" by these. (Venâncio, 2021, p. 90)[19]

2. The Council of Europe - Budapest Convention on Cybercrime

Mainly in last decades, the globalization has promoted a higher and effective evolution in all dimensions of the Human life around the world. There are multiple study and analysis perspectives, being sure that the balance between positive and negative effects must be seriously identified and worked by all actors, especially those who have the different powers and roles in the society – national(s) and/or international. "*The idea of global citizenship as a facet of national citizenship … extremely important. (…) nation states enjoying reasonable stability, affluence and commitment to Human Rights and democratic principles play a crucial role in mainstreaming international institutions and promoting international agreements."* (Carter, 2001, p. 204) However, those states that doesn´t accept or implement the Human Rights and, consequently, doesn´t ensure or protect by law, political governance and justice must be in the top of International Community aiming to enforce law and promote elementary positions and

[13] Pedro Dias Venâncio, (2021), in *Tipos Legais de Crimes Informáticos*, Cibercriminalidade – Novos desafios, ofensas e soluções – Coordenação de Inês Sousa Guedes & Marcus Alan de Melo Gomes – Edição: PACTOR – Edições de Ciências Sociais, Forenses e da Educação – Lisboa – Portugal.
[14] Pedro Dias Venâncio, (2021), in *Tipos Legais de Crimes Informáticos*, Cibercriminalidade – Novos desafios, ofensas e soluções – Coordenação de Inês Sousa Guedes & Marcus Alan de Melo Gomes – Edição: PACTOR – Edições de Ciências Sociais, Forenses e da Educação – Lisboa – Portugal.
[15] *Idem.*
[16] *Ibidem.*
[17] *Ibidem.*
[18] *Ibidem.*
[19] *Ibidem.*

changings to promote the International Security. In this context, the International Organizations, as the *Council of Europe*, have been doing a hard but important work – legal, political, social, economic – to increase the whole protection of Human Rights, preventing and combating international crime and, consequently, the International Security.

It´s obvious that with the globalization the internet has "explode" around the world and there is an undeniable dependance. Recent statistics state that 1 in 4 people around the world are connected in the cyberworld, being predominantly depending on it. This is an unmatched evolution of the technologic systems, affecting life and structures in all dimensions in global context. However, this "new" world generated new crime opportunities, strategies and with the severest damages to everyone and to all structures or institutions, mainly the Cybercrime. This is one of the most dangerous threats to the Humanity, to the International Community and to the Nations and States. The Rule of Law, the democracy and the Human Rights have been the most negative affected with the threats by offences and damages using means of computer systems. This means that international peace is affected and in danger by the impact of the cybercriminal actions. The economic and the financial systems have been seriously affected with the hardest consequences to the States and societies. The International Law and the States Law have developed the legal answer – Juridical and Judicial – there are criminal investigation and policies (re)action, but the mechanisms, instruments and modus operandi used by the Cybercriminal are in permanent change and evolution that represents the hardest difficulties to catch the criminals and to identify the means and proceedings of implementation of their action. The emergent need is to keep the internet a safe "place" and protected, by the law, by the justice and by the political powers response but all constraints are the real challenge.

So, as one of the nowadays biggest problems faced by States, Institutions, and individuals, all around the world, the Cybercrime is not a new concept or a new way to practice International Crime, but it has increased in dimensions that we can affirm that are out of control of the national, regional, and international political, legal, economic, financial, cultural, and social control. The prevention and the combat against Cybercrime have been developed in different contexts and by the most different parties involved, using the multiple and most diverse strategies, by the vanguard leading edge technologies, mechanisms, and instruments, constantly changing and undetectable by the security systems, including the most advanced.

In fact, there is a global concern and a network system being permanently developed and assumed by the States, International Organizations and by the individuals. All of those who are in Internet world are real victims or potential victims.

In the International and in many national frameworks, the legal systems that recognize the Cybercrime has been implemented and developed, in straight connection with the judicial systems that has been adapted to this reality although the inherent serious difficulties in denouncing, judge and punish the criminals. Mainly as consequence of the cybercrimes committed, the damages caused to individuals, States, companies, Organizations and Institutions of all areas, the prevention and the combat against Cybercrime has been putted in the top of the agenda of the International Community and the Governments. The study case of this paper is about the one of the most active International Organization in this prevention and combat aiming to achieve to a global scope: the *Council of Europe*.

The *Council of Europe* has been one of the most relevant and active International Organization, having a fundamental role within the international law and criminal justice, by the *Budapest Convention on Cybercrime* (2001), the *First Additional Protocol on Xenophobia and Racism* (2003), the *Second Protocol to the Cybercrime Convention* (expected in Spring 2022) and by different treaties on International Criminal Justice. The main strategy adopted by the Council of Europe, by the legal and political documents and procedures, is always based in the International Cooperation, not only between and to their members, but with different States invited to participate and sign the International Legal

documents.[20] In the pursuit of this challenge, the *Council of Europe* has a *Cybercrime Convention Committee (T-CY)*[21], having representatives of the Parties and responsible for assessing proper implementation of the *Budapest Convention on Cybercrime* and the *First Additional Protocol on Xenophobia and Racism*.

With the same objective, the Council of Europe has been developing different projects, namely the *Cybercrime Programme Office of the Council of Europe (CPROC)* to assist countries all around the world to "*strengthen their criminal justice capacities for the investigation, prosecution and adjudication of cybercrime and other cases involving electronic evidence in line with the Convention and recommendations of the Cybercrime Convention Committee (T-CY)."* (Council of Europe, 2022)

Along the last more than two decades, the *Budapest Convention on Cybercrime* remains the most relevant international legal instrumental in the International Law. Criminalizing the offences against and by electronic means, the Convention defines the procedural tools to secure the electronic evidence, promoting the International Cooperation between Parties. More than a treaty this Convention develop strategic procedural powers and mechanisms based on the International Cooperation against any offence through electronic means. There is a relevant neutrality concerning the technology that allows to answer of multiple complexes challenges the cybercrime imposes along these twenty years.

The increasing dependance on global computer networks shows the vulnerability of all users – private, institutional or government – to the cybercriminal action. "*The rise of technology and online communication has produced an increase in the incidence of criminal activity, and it has also resulted in the emergence of what appears to be some new varieties of criminal activity. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.*" (Csonka, P., 2003, p. 473). So, the *Council of Europe* in the pursuit of the permanent prevention and combat against Cybercrime promote different projects and meetings to promote and evaluate the legal procedures under *Budapest Convention on Cybercrime*. In last November 2021, there was a relevant meeting: the *Secretariat of the Cybercrime Convention Committee (T-CY)* with the support of different Projects - *OCTOPUS, GLACY+, iPROCEEDS-2, CyberEast and CyberSouth* – the 24/7 Network of contact points established under the *Budapest Convention on Cybercrime*.

This meeting has the main objective to debate and ensure the implementation of the Article 35 of the Convention, mainly the responsibilities of the 24/7 Network, "*the provisions on technical advice, collection of evidence, provision of legal information, and locating of suspects, as well as the challenges of implementing new responsibilities under the forthcoming Second Additional Protocol to the Convention and possible capacity building support for the members of the Networ*k." (Coe, 2021 *Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime – Summary Report*[22]). With more than 80 participants, representing states from all continents, there are some relevant discussions and conclusions that need to be pointing out. During 2021, the progress and support provided by the countries have been considered globally as positive, considering the needs and the possible reply – by governments and institutions according to the legal procedures preview in the

[20] After the invitation presented by the *Council of Europe, Congress of Brazil approves accession to the Budapest Convention*: "*On 15 December, the Senate of Brazil approved accession to the Budapest Convention. This crucial step will permit the Government of Brazil to deposit the instrument of accession and become a Party to this treaty any time soon, and thus to cooperate effectively on cybercrime and electronic evidence with currently 66 other Parties. Brazil is now also a priority country for capacity building and tailor-made technical assistance activities for criminal justice authorities will be further enhanced*." (Council of Europe, 16 Dec. 2021) in https://www.coe.int/en/web/cybercrime/-/congress-of-brazil-approves-accession-to-the-budapest-convention.
This is very important to implement and to the evolution of the International Cooperation of the prevention and combat against Cybercrime. Until now, this Convention was ratified by almost 70 States, that is very important.

[21] This Committee is permanently preparing and developing Guidance Notes and additional legal instruments and facilitating cooperation among the Parties.

[22] *Council of Europe, Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime*, 24 November 2021, Summary Report, in https://www.coe.int/en/web/cybercrime/home.

Convention. By other side, it was discussed the near future need to face seriously the inherent challenges in beginning of 2022 - the approval and implementation of the *Second Additional Protocol to the Convention on Cybercrime.* There will have a hard work to develop to promote the legal measures in practice to prevent and combat the Cybercrime. Third main point of this Meeting was the activities jointly organized with INTERPOL, under the International Cooperation strategy of the Council of Europe and specially under the Convention, promoting the need tools and channels, aiming being the answer to the International Security (re)action(s) in dully time.

Along the meeting there were detailed and important discussions, in the same measure of the importance to evaluate and ensure the Convention implementation, but particularly the emergency of the adaptation the measures to the reality of the strategies of the action of the Cybercrime, prevent the damages and violence that are out of control in too many dimensions. Concerning the Justice, it´s urgent the develop and execution of safety actions by national and international authorities, identify and apply the judicial procedures to judge the criminals. It was presented several proposals, dedicated to the international cooperation on cybercrime, within the need of the need of training to put the programs and the projects in practice.

The conclusion of this meeting, as the aim of the Council of Europe in general, and the prevention and combat to the Cybercrime in particular, is a focus position by all that the problem is growing and in all areas of human and states lives, the laws and justice procedures have to be in permanent adaptation to the permanent evolution of this crime and modus operandi of these criminals, being sure that the main key of the challenge to the International Security is the International Cooperation under the international legal documents, specially the Budapest Convention on Cybercrime and all follow legal instruments and mechanisms.

CONCLUSION

In face of the exponential growing of the utilization of the technology and the internet, persons with deviant behaviors use these means to practice the criminal activities. It´s evident at a worldwide level the enormous evolution and growing of the criminality associated to these instruments and mechanisms of work and leisure, so, it was mandatory that International Organizations and States react to combat the cybercrime.

Our research work demonstrates how the Council of Europe, by the Budapest Convention on Cybercrime, and the Portuguese State, by the creation of the Cybercrime Law, developed Crime Policy instruments. All of these are essential to prevent and combat properly those deviant behaviors.

REFERENCES

1. Center, A. 2001. The political theory of Global Citizenship. Roudledge.
2. Council of Europe, Cybercrime - https://www.coe.int/en/web/cybercrime/-/congress-of-brazil-approves-accession-to-the-budapest-convention.
3. Council of Europe. 2001. *Budapest Convention on Cybercrime*.
4. Council of Europe. 2003. *Budapest Convention on Cybercrime* - First Additional Protocol on Xenophobia and Racism.
5. Csonka, P. (2003). The council of Europe's convention on cyber-crime and other European initiatives. in Revue internationale de droit pénal. 2006, n. 3-4. Vol. 77. pp. 473-501. https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-473.htm?contenu=resume.
6. Steve Morgan, Editor-in-Chief, in Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybercrime Magazine, Sausalito, Calif. (Nov. 13, 2020) https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, consulted in 2022-01-27.
7. Internet Crime Report-2020, FBI/IC3 – Federal Bureau os Investigation/ Internet Crime Complaint Center - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
8. ITU (International Telecommunication Union). (2019). Measuring Digital Development: Facts and Figures 2019. Geneva: ITU. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf , consulted in 2022-01-27.

9. Kemp, S. (2019). "Digital 2019: Global Digital Overview". Datareportal. https://datareportal.com/reports/digital-2019-global-digital-overview.
10. Lei n.º 79/2021, de 24 de novembro, pode ser feita no site da Procuradoria-Geral Distrital de Lisboa do Ministério Público no link - https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3476&tabela=leis&ficha=1&pagina=1&so_miolo= .
11. Lei n.º 109/2009, de 15 de setembro, pode ser feita no site da Procuradoria-Geral Distrital de Lisboa do Ministério Público no link - https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis .
12. Marques, G. & Martins, L. – 2006 – Direito da Informática (2.ª Refundida). Coimbra: Almedina – Portugal.
13. Pedro Dias Venâncio, (2021), in *Tipos Legais de Crimes Informáticos, Cibercriminalidade – Novos desafios, ofensas e soluções*. Coordenação de Inês Sousa Guedes & Marcus Alan de Melo Gomes – Edição: PACTOR – Edições de Ciências Sociais, Forenses e da Educação – Lisboa – Portugal.
14. Statista 2022 - Data breaches worldwide 2020, by victim industry and size - Published by Joseph Johnson - Jun 4, 2021 - https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/
15. *The Global Risks Report 2020* - 15th Edition, of the World Economic Forum In partnership with Marsh & McLennan and Zurich Insurance Group - https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf .