UNIVERSITY OF NEBRASKA- LINCOLN **U.S. STRATEGIC COMMAND**

2018 DETERRENCE AND ASSURANCE ACADEMIC ALLIANCE CONFERENCE,

"Thinking Outside the Silo:

Creative Problem Solving in Deterrence and Assurance"

- THE DRAFT CYBER-ARTICLES ON DIGITALIZATION OF HUMAN RIGHTS –

***Aleksandar Tashkovski*, LL.B.**
LL.M. Student in International Law
and Relations and Law of the European Union
Faculty of Law "Iustinianus Primus"
Ss. Cyril and Methodius University in Skopje
R. Macedonia

ABSTRACT

Each generation of people is a witness of its own case about the direction of mankind's evolution. The course that we will take speaks for the level of consciousness that we have. In the last two decades of our time we have seen rapid development of technology and science at a speed much faster than the capacity of people to internalize the benefits from these discoveries. The fact that we live in an era of information and globalization enabled scientific revelations, and with the help of the internet to get to the peoples from underdeveloped/developing/transitioning countries, we cannot state the same for the benefits and blessings that come from the usage.

Cyberspace allowed people to not just connect faster and easier, have access to all kind of information, but also to close themselves in the electronic devices and become "one" with them. So, today we can talk about a different kind of people: electronic or cyber- human. No one can imagine how our ordinary day would look without the benefits from the cyber evolution. From here springs up the need for defining a fourth generation of human rights that are crucial for our future development- cyber rights of people.

But, in the same time, men continue to repeat the mistakes from the past, regardless of the level of technology development. That is why we are witnessing massive abuses of the knowledge that enabled the existence of cyber technology, i.e. all the forms of abuse that can pop up in our daily lives and relate to electronic device or internet. Even in criminal law a new sub-branch has developed- cybercrime.

This brings us to the conclusion that the integration of cyberspace capabilities and the toolkits for deterrence already exist. The thing that we must discuss is how to improve and upgrade this toolkit not just to deter people, but to establish an international legal regime which will offer a long-term solution for eradication of the mentality of abusing the common interest of people (cyberspace) for personal, selfish and low lucrative interests.

The thesis that this research will present is that the viability of cyberspace is impossible without a deterrence toolkit and will present the proposal for an international legal regime. The methodology that will be used will be pure legal research with comparative legal analysis. The national legislation regulating cyberspace of the 7 most developed economies in the world (G-7 group: USA, UK, Japan, Italy, Germany, France, Canada) will be analyzed. Also, international sources (with special accent on the Budapest Convention on Cybercrime) that regulate the materia of cyberspace will be evaluated. The

conclusion will offer recommendations and measures that need to be taken to upgrade and improve the deterrence toolkit for cyberspace capabilities in national and international level depicted in a proposal for the aforementioned legal regime.

TABLE OF CONTENTS

I. INTRODUCTION

The cyber- mania, defined by Mary Ellen O'Connell[1], has its own reasons for existence and reasons why it is manifesting precisely in this form, as: mania. Mania as a psychological state of the human mind presents a mental illness that manifests as a sick obsession with an idea and is characterized with abrupt changes from state of euphoria to depression and reverse, or its other manifestation: obsession, which means having a big passion or wish for something[2].

The source for this mania should be investigated in the human mind, and the implications to the human psyche from the digitalization of human existence shall be left for analysis and elaboration to the respected professionals from the appropriate scientific disciplines. For them to have an empiric answer to the above settled question, it is crucial for the digitalization to happen in some territories in its full potential for the respective scientist to be able to declare their findings, with goal to be implementable in the law theory dilemmas. The implications toward the human mind are especially important because they provide help for the determination of the human intention in the cyber place, which can easily be incriminated and with it placed under the jurisdiction of the criminal norms that investigate the human intentions, which automatically brings the investigation of the human will.

Regardless, the Cyber (or Internet, or digital, or any other word derived from the essence of the research subject that here we try to elaborate in words) era has started in 1969, but the same cannot be stated for the Internet revolution, because there is no equal enjoyment from all people and states from the world, of the benefits from the Cyber era. At the same time, its second period is at our doorstep (from the Cyber era)- the time when every human being will want its own robot, while the full enjoyment of the benefits from the Internet are not yet fulfilled. That is why the Informatic or Cyber revolution can be properly analyzed only when there will objectively be equal opportunity and chance for self- digitalization.

But, the mania that we previously mentioned, does not have to represent a psyhic disease, but also a right willfulness, passion and desire for science and the benefits that come with it, in the concrete case from the information technologies.

---

[1] Mary Ellen O'Connell, International Law: Meeting Summary, Cyber Security and International Law, Chatham House, 29 May 2012

[2] http://makedonski.info/show/манија

In that context, "the stubs of the information technology are the first mechanical machines, created for conducting mathematical operations, which is the case with the abacus from Asia. The first computer capable of conducting different operations with specific commands (programs) is ENIAC (Electronic Numerical Integrator and Calculator), created in USA from 1947. The development of the Internet dates back from 1969, from the so called APRAnet (Advanced Research Project Agency), organization for network research, established from U.S. Department of Defense. The goal of this network was to allow its users direct access to powerful computers based on few universities and laboratories. In the same time, with APRANet different computer networks were established (BITNET, CSNET, FIDONET, USENET). Like this, after 1970 the NCP (Network Control Protocol) was established that allowed connection of more computer networks. The name Internet was established in 1982 with change of NCP with new Transfer Control Protocol/ Internet Protocol (TCP/IP). The most popular service of the Internet, the World Wide Web (www) occurs in 1992"[3].

With the creation of virtual network through which every computer can access and connect with other computers in a virtual process from which humans can have different benefits on different grounds and everyone who has access to a computer can enjoy these benefits. Namely, we are speaking about the creation of res communis omnium from ex nihilo.

The long debated and announcements of the fourth generation of human rights, which some authors also define as Communication rights[4], present neither more nor less, but article 27 from the Universal Declaration of Human Rights: "Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.". This stipulates the right to freely enjoy the benefits from science, arts and cultural life. Cyber law, just like Telecommunication law, Space Law, Bio-medicine Law and other (wave of) branches that developed, will follow this trend in the future with different fluctuations (proportionally with the scientific development), parallel with the evolution of the human mind and its focus on science and art, their proper academic investigation and creation of new findings.

[3] Гоце Наумовски, Дајан Роуланд, Јута Кол, Ендрју Чарлсворт, Право На Информатичка Технологија, Скопје, pg.9-10 (2013)
[4] Nouri Neshat, Saeid, Communication Rights: Fourth Generation of Human Rights, (2003)

In meantime, the legal thought must not underestimate the dignity of the development of other scientific and artistic fields, and that is why it is crucial to approach to analysis of the benefits from the progress of Science and Arts as one, to investigate their possible intersections with the legal sciences, with the goal to establish fair distribution of the benefit that man came to through the progress of Science and Art, also for more pragmatically identify and predict possible future legal scenarios.

The fact that some scientific or artistic findings are in the twilight zone of their discovery, while others are in sight, does not mean that they will not be treated with a respective legal regime, or as is the case with the jurist thought for the legal regime of outer space, that can be traced back to 1932[5], way before Science had any discoveries or findings about outer space travel. Regardless of that developed jurist thought, the "Outer Space Treaty was drawn up not in some haste within the space of less than 12 months, but also less than ten years after the launch of the earth's first artificial satellite"[6].

Electronic devices that humans use daily, present an inseparable part of the progress of science and with it, of humanity. Creating a competition for digitalization in all spheres of the human existence, economy, society, state, international and human relations, by virtualization of the digital world from the cyber place in the objective reality of our existence, it establishes the constitute contours of the self-maintained cyber human, who will not rest its existence and security on the Social Agreement only, but on the opportunities from the cyber place too. The danger rises when the cyber human, by receiving power of information and knowledge, will start to live in the visualization of wrong self-destructive worship that leads to the danger of creating sloppy human beings without being self- initative and conscientious about the world around and in themselves, because of the obsession with its own destructive worship that, if practiced by many, results with the reduction of the human evolution and progress.

II. CYBER LAW

The process of human behavior regulation in the context of the benefits from the scientific and artistic progress is proportionate to the power that comes with that finding and the danger of its abuse from low human lusts that obsess and effect negatively on the

[5] V. Mandl, Das Weltraum- Recht: Ein Problem der Raumfahrt (1932)
[6] B. Cheng, Space Objects and Their Various Connecting Factors, in Outlook on Space Law over the Next 20 Years (Eds. G. Lafferranderie & D. Crowther), pg. 203 (1997)

human mind. That is why scientific disciplines, such as the information technology and engineering, whose development automatically generates a legal discipline that investigates the power that may be abused and affect human existence negatively; and at the same time is a generator of human rights. This is the paradox of Cyber Law.

In this research, we will not investigate whether Cyber Law is Law at all, or a branch, an area, a discipline, but we will rather settle its existence from the social reality of the benefits from the scientific development of the respected scientific discipline.

Namely, the first cyber- regulation occurred in Germany in 1970[7], at the same time with the term "Information technology (IT) that arose during the 1970s to describe the combination of two previously existing disciplines: computing and telecommunications"[8].

As an independent legal discipline, along with specialized IT Law studies, it is implemented in many Universities around the world. Parallel to the development of the information technology industry, the positive law of developed countries where this industry exists has developed, and with it cyber law in general.

Consider the fact that "from 2000 to 2008, the Internet has expanded at an average annual rate of 290 percent on a global level, and currently an estimated 1.4 billion people are connected to the Internet, which is close to 25 percent of the world's population. The technology has advanced so fast and has become more and more user friendly; at the same time, people around the world have become more and more sophisticated in the use of technology"[9].

The legal doctrine investigates Cyber Law in a manner that many authors[10] make similar systematization of cyber space research, dividing the investigation in chapters such as: cyber-criminal, responsibility and liability of states, e- commerce, domain names, intellectual property rights, e-correspondence, e- agreements, trademarks, military cyber law, virtual worlds, taxes, proofs, ethics, privacy, freedom of expression, data protection,

[7] Гоце Наумовски, Дајан Роуланд, Јута Кол, Ендрју Чарлсворт, ПРАВО НА ИНФОРМАТИЧКА ТЕХНОЛОГИЈА Скопје, pg. 11 (2013)
[8] Chris Edwards, Nigel Savage, Information Technology& The Law, pg. 1 (1986)
[9] Zeinab Karake Shalhoub and Sheikha Lubna Al Qasimi, Cyber Law and Cyber Security in Developing and Emerging Economies, pg. 1 (2010)
[10] Jeff Kosseff, Jonathan Rosenoer, Mark F. Grady, Francesco Parisi, Robert Dunne, Diane Rowland, Elizabeth Macdonald, David Bainbridge, Ian J. Lloyd, Michael N. Schmitt, Chris Edwards, Nigel Savage, Ian Walden, Diane Rowland, Andrew Charlesworth, Uta Kohl, Goce Naumovski…

protection of human rights. In essence, the doctrine investigates the practical aspects from the benefits of the development of the information science.

II.1. CYBER CRIMINAL

"It has been reported that, since 1993, attacks on the computer systems of banks and other financial institutions, made possible by the use of the latest generation of military weapons which target communications systems, have resulted in losses in excess of £500 million as the organizations involved pay 'ransom' money"[11].

One of the characteristics of the Law is its capability of having an insight in other scientific and artistic fields, with it regulating their existence or determine their self-regulation. Like that, the criminal deeds done in the cyber place present an interdisciplinary area by itself that incorporates Cyber Law and Criminal Law (national and international criminal law). For detailed elaboration on the intersection between the International Humanitarian law and Cyber Law, determination of state responsibility and wrongful cyber-attack, see: Michael N. Schmitt-Tallinn Manual on the International Law Applicable to Cyber Operations-Cambridge University Press (2013) and (2017).

"As more aspects of our life move to digital networks, crime comes with them. Our lives increasingly depend on the Internet and digital networks, but these create new vulnerabilities and new ways for criminals to exploit the digital environment. Not only can many existing crimes be replicated in online environments, but novel crimes that exploit specific features of digital networks have emerged as well. With new crimes come new forms of policing and new forms of surveillance, and with these come new dangers for civil liberties"[12].

The being of the criminal act or corpus delicti of cyber-criminal deeds presents a "sum of the special elements (characteristics, that can be from objective- action of executing, consequences, and from subjective nature- intent, goal, motive) that characterize that criminal act, separating it from other criminal acts, or in other words it presents the core of unlawfulness"[13]. Corpus delicti of cyber-criminal acts presents an abuse of the scientific progress of information technology.

---

[11] Diane, PhD. Rowland, Elizabeth MacDonald, Diane Rowland-Information Technology Law, pg. 447 (2000)

[12] J. M. Balkin & Jack Balkin & James Grimmelmann & Eddan Katz & Nimrod Kozlovski & Shlomit Wagman & Tal Zarsky, Cybercrime- Digital Cops In A Networked Environment,

[13] Ѓорѓи Манојловиќ, Методија Каневчев, Македонско Кривично Право општ дел седмо, изменето и дополнето издание, pg.96-97 (2010)

The object of the criminal act or the protected object "is not object in a material sense, but a value; protected objects secures the highest values of the society upgraded as law institutions."[14]. The protected object in the cyber- criminal law is different for every different cyber-criminal act.

The subject of the criminal deed is of course men, but in this context, we have to mention that cyber deeds do not present 'delicta propria', since they do not require characteristics form personal (adult, parent, siblings) or official manner (military or bureaucracy official) in order for the criminal deed to be realized access to information technology today is not that limited; but on the contrary they are 'delicta comunia', with only one specific- the criminal will need to have access to computer.

Types of cyber- criminal deeds can be manifested in different kinds, their visualization i.e. manifestation from the digital in the real world will depend on the creativity and skills of the executor, so we can find: identity theft, e- cards theft, securities, interruption in computer or telecommunication service, computer espionage, hacking, distribution of malware, other kinds of malicious software, stalking, production and distribution of illegal porn, cyber terrorism, digital piracy, abuse of personal data, unauthorized use of finding or software. The list will be increasing in proportion with the development of information technology and engineering.

II.2. THEORIES OF CYBERSPACE REGULATION

"Government actors in many countries attempted to react to the Internet using conventional means of the state apparatus, like passing laws in parliament or having courts judge over access to unlawful content. In most cases this proved to be fruitless; in fact it demonstrated the weakness of the traditional nation-state in attempts to regulate the Internet. Just to give a few examples: since 1997 there has been a law on digital signature (the oldest in the world) in Germany, but after seven years there is still no practical way to sign a contract on the Net. In several countries, courts have attempted to punish Internet service providers (ISPs), which allowed access to hate speech or child pornography for example, usually without any success. True, there are governments like

[14] Ibd. Pg.98-99

Singapore or China that censor content on the Net, but the effect is limited as the fluidity of the Net often means that filtering programs can be circumvented."[15]

That is why the subtitle is theories, not real regulation of Internet.

Debates go from regulation, to self-regulation and co-regulation. Special interest has been evoked by Lawrence Lessig[16] regulatory model who introduces the model of factors i.e. modalities of regulating that do not have to be laws (direct regulation) only, but other factors or limitations that can affect human behavior, for example the social norms (they control human behavior and with it impose its regulatory effect), market (prices affect the lifestyle of people), and the code- architecture (the physical world around us that has consequences on human behavior). Indirect regulations, as previously mentioned, are influencing on a subconscious level, humans are rarely aware of their existence, unlike the direct regulating. In that regard, we can see that the Lessig model gives more possibilities for regulating, and in that context the proposed legal regime draws inspiration from this model also.

For easier understanding and augmented debate for the theories of cyber regulation and their usage justification from regulators around the world, first we need to understand the legal nature of the Internet whose interpretation has to start with the sources of cyber law.

II.3. LEGAL CYBER LAW SOURCES

Sources can be grouped in formal and material (that can be written or unwritten (custom law)) ones. The same division can be applied on domestic and international level.

First, we will approach with the legal norms that are above the national legislature- the International Law.

II. 3.1. INTERNATIONAL SOURCES

In that line, unfortunately, on an international level we can find a mixture of different entities who all create soft cyber law, such as: specialized agencies of UN (International Telecommunication Union, its specialized agency International Multilateral Partnership Against Cyber Threats and World Intellectual Property

[15] Self-regulation, Co-regulation, State Regulation, Hans J. Kleinsteuber, The Internet between Regulation and Governance

[16] Lawrence Lessing, Codes and Other Laws of Cyberspace, 1999, New York Basic Books and version 2.0

Organization) Internet Corporation for Assigned Names and Numbers (nonprofit, includes Internet Assigned Numbers Authority (IANA), that established the International Ad Hoc Committee (IAHC) whose mandate expired and it stopped with work), The Internet Society (non-profit, includes: Internet Architecture Board), International Trademark Association (nonprofit), Information Working Group of the Asia- Pacific Economic Cooperation forum, Association of Southeast Asian Nations (ASEAN) which engages for information infrastructure among its member nations, Forum of Incident Response and Security Teams (FIRST) is an international federation of individual CERTs, The Organization for Economic Cooperation and Development Working Party on Information Security and Privacy (WPISP), The Institute of Electrical and Electronic Engineers (IEEE) is a professional association , The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), through a joint technical committee (JTC), have developed information security standards, The Internet Engineering Task Force (IETF) is a technical standards-setting body, the Meridian Conference and Process aims to exchange ideas and initiate actions, INTERPOL, NATO and others[17].

Because of this, we will first approach to a teleological interpretation of the legal nature of Cyber Law through International Law. For that to be done, we will need to define the material sources of the same, and that is- the Internet, as a prerequisite of the existence of this discipline. Namely, the internet network presents a 'res communis omnium', because of that its appropriation is forbidden. It is a legal principle that finds its suitable adjustment use as commons or common heritage of mankind, found in the Outer Space Treaty, Antarctic Treaty and Law of the Sea. "According to the common heritage of mankind concept certain areas outside national jurisdiction containing valuable resources not only should be considered not appropriable by States, but also, they should be managed by all States acting collectively and exploited for the benefits of all States, taking into particular consideration the needs of the less developed ones. One of the major problems emerging as a controversial issue of international law with regard to the common heritage of mankind concept is the difficulty to arrive to a clear and generally accepted definition of its meaning and legal value. Despite the fact that the 'Common Heritage of Mankind' has received normative recognition in several legal

[17] List of some organizations: https://cybersecurityventures.com/cybersecurity-associations/

instruments, none of those provide a clear-cut interpretation of its nature and legal consequences."[18]

There is a difference between the common heritage of mankind concept and the commons concept. In that regard, the common heritage of mankind concept requires the establishment of an international legal regime, while the commons concept does not require an international regime, and as it can be seen in the concrete case, the establishment of such regime is contrary to the legal nature of the internet.

Practically, from the way of creation and establishment of the functionality of the Internet (its definition) it has defined and crystalized the leading legal principle of Cyber Law and that is its commons. Namely, the defining of the internet as commons or as 'res communis omnium' is officially made for the first time from the official delegate of Malta[19] on the World Summit on Information Society Review Process, held in New York, 15 December 2015 .

Like this, the foundation of the legal principle that established the 'res communis omnium' of cyber place, created from ex nihilo, in form of benefit from science (information technology and engineering) that present 'sui generis' commons. It is interesting how the application of this principle in Cyber Law does not require the establishment of any international legal regime that will guide the usage of this commons, but on the contrary, it presents a regime for itself, by itself, who is on a track of a never-ending upgrade and will continue to develop in that perpetuum mobile direction.

Equally important is the understanding of the prohibition for regulating things that are 'res communis omnium', a term that finds its roots from Roman Law[20] and it proofs the existence of human consciousness for the commons. In today's context, that means that cyber place is no one's property and now one can appropriate it. In this part, Cyber Law has connecting spots with Space Law, regarding the legal principle of non-appropriation of outer space (Outer Space Treaty, art. 2), the legal principles for freedom of exploration and use without discrimination (art. 1) also the principle for cooperation and mutual assistance (art. 9) can be considered.

---

[18] Fabio Tronchetti, The exploitation of natural resources of the moon and other celestial bodies: a proposal for a legal regime, pg. 86-87 (2009)

[19] https://www.academia.edu/19974250/Protecting_the_Internet_as_Common_Heritage_of_Mankind

[20] Justinian codification: "By the law of nature these things are common to mankind: the air, running water, the sea, and consequently the shores of the sea." VI- th Century C.E."

The establishment of an international legal regime for the commons and common heritage of mankind would inevitably lead to the foundation of perpetual peace among States and peoples in the world.

A big number of instruments has been adopted on regional, but not on international level. So, the EU has its own instruments for international private law (Brussel and Rome Regulation), and for concrete areas (privacy, cybercriminal, e-commerce, intellectual property rights, domain theft, human rights): General Data Protection Regulation replacing EC No. 95/46, Directive on Data Protection in 2016, OECD Transborder Flow of Data (1980), Convention on Cybercrime (The Convention is the first and only multilateral treaty to address computer-related crime and evidence gathering. It imposes obligation for criminalizing certain conducts from cyber space, creates investigative procedures, collecting e- evidence, establishing a broad international cooperation regime including extradition), Community Framework for Electronic Signatures 1999/93/EC, United Nations Convention on the Use of Electronic Communications in International Contracts (UNCITRAL has also issued the UNCITRAL Model Law on Electronic Commerce, 1996 (MLEC), followed by the UNCITRAL Model Law on Electronic Signatures (MLES), 2001), Berne Convention for the Protection of Literary and Artistic Works, Uniform Domain Name Resolution Policy, Madrid Agreement and Protocol, and human rights instruments.

The evolution of the legal texts leads us to the conclusion that the period of complete ambiguity is overcome and the foundation for creating an international legal cyber- instrument is settled.

But regarding Public International Law, the international customs are of tremendous importance (custom as explained above is part of the material sources of the Law). State practice and 'opinio juris' are the parameters that need to be cumulatively fulfilled for the custom to become reality. In International Cyber Law context, opinio juris has not been established[21]. State practice unfortunately is not fully practiced in light of the self-established legal principles of cyber space, which is why today there are still States that are enemies of the Internet or are under surveillance or have no data at all[22]. We cannot speak for a constitution of an international custom that is unlawful and

[21] http://www.un.org/sustainabledevelopment/blog/2017/07/half-of-all-countries-aware-but-lacking-national-plan-on-cybersecurity-un-agency-reports/
[22] https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country

contrary to its legal principles, declaring the digital commons as state sovereignty. 'In re' digital commons that presents an international wrongful act of the States that are conducting this and it gives grounds for processing a claim in front of the International Court of Justice for breaching 'erga omnes' obligation of States. The protection from discrimination that States must conduct on the territories where their jurisdiction is practiced applies to the digital commons also, therefore States who are enemies of the internet are practically enforcing discrimination for its own citizens in the process of using the benefits from this common and bear international responsibility for that.

II.5. CYBER LEGISLATIVE OF G-7 COUNTRIES

In manner of G-7, it is important to mention that while the group of seven was the group of eight, the creation of the G8 Subgroup on High-Tech Crime was established, which seeks to prevent, investigate, and prosecute crimes involving computers, networked communications, and other new technologies was established. Afterwards, in 1997, the subgroup created the 24-7 High-Tech Crime Point-of-Contact Network, which lets law enforcement officials from countries-including those from outside the G8-quickly contact their counterparts in other participating nations for assistance with cybercrime investigations.[23]

II.5.1. United States of America[24]

The internet era was created and started from this country, so it is logical to have a developed legislature network for this area, especially because of the democracy tradition and stable legislature. In that context, the USA has brought a lot of national laws that regulate cyber space, part of them on federal level:1996 Health Insurance Portability and Accountability Act (HIPAA), 1999 Gramm-Leach-Bliley Act, 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA), 2015 Cybersecurity Information Sharing Act (CISA), Cybersecurity Enhancement Act of 2014, Federal Exchange Data Breach Notification Act of 2015, National Cybersecurity Protection Advancement Act of 2015; and another part it can be found in the legislature

[23] https://www.networkworld.com/article/2231519/security/who-really-sets-global-cybersecurity-standards-.html?page=2
[24] https://www.loc.gov/law/help/guide/federal.php

of the states that consists the USA, in that manner New York and California have developed their own national legislature for this area.

II.5.2. United Kingdom[25]

UK follows the step of USA regarding cyber-regulation and adds up with its long democratic tradition, translating long-term regulation solutions not just for cyber space, but other areas also. The cyber- regulation is consisted from more instruments, including, but not limiting to: Computer Misuse Act 1990, The Public Telecommunication System Designation (International Computers Limited) Order 1998, No. 3013, The Chessington Computer Centre Trading Fund (Revocation) Order 1996, No. 1995, ,The Chessington Computer Centre Trading Fund Order 1993 No. 948, The Copyright (Computer Programs) Regulations 1992, No. 3233, The Copyright (Computer Software) (Extension to Territories) Order 1987, No. 2200, Act of Sederunt (Computer Evidence in the Sheriff Court Amendment) 1970 No. 456 (S. 28), Act of Sederunt (Computer Evidence in the Court of Session Amendment) 1970 No. 455.

It is important to mention that the definition of the cyber terrorism and its classification as a national security was first done in this country.

II.5.3. Canada[26]

Within Canada there are three general (and broad) forms of law that regulate security and privacy in Canada: the federal PIPEDA (Personal Information Protection and Electronic Documents Act, PIPEDA is its abbreviated name), the provincial variation of PIPEDA in Alberta, and certain health information acts. ("PIPEDA"). British Columbia and Quebec have similar legislation. But what is worth mentioning is that, in similar way to USA and UK, Canada has a whole operational support system that is interconnected and helps citizen to be cyber- secure.

In that manner cyber security is regulated on federal and provincial level, executed from more organs, such as: Communications Security Establishment Canada (CSEC), Royal Canadian Mounted Police, Canadian Security Intelligence Service, Department of National Defense, Industry Canada, Defense Research and Development

[25] https://www.legislation.gov.uk
[26] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx and http://laws.justice.gc.ca/eng/

Canada, Treasury Board Secretariat, Shared Services Canada, Canadian Radio-television and Telecommunications Commission, Office of the Privacy Commissioner of Canada, Canadian Anti-Fraud Centre,

II.5.4. Japan[27]

"In Japan, privacy and data security law largely is governed by a 2003 statute, the Act on the Protection of Personal Information (APPI). The statute is more similar to the comprehensive EU approach to data regulation, and certainly is more stringent than the U.S. sectoral approach. Indeed, Japan's privacy and data security protections are among the most comprehensive in Asia.

Among the notable features of APPI is its relatively broad definition of "personal information" that is protected by the statute. APPI defines "personal information" as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will enable the identification of the specific individual."

Japan's privacy and data security laws, like those of Europe, suggest that personal information protection is a human right. APPI sets for a general "basic principle" that companies should cautiously handle Japanese residents' personal information "under the philosophy of respecting the personalities of individuals.[28]"

The legislature of France, Germany and Italy shall not be conducted, since all three are member states of the European Union and the above elaboration for the EU cyber-legislative is a source of Law in these countries also.

III. CONCLUSION

The Internet phenomena dates back in 1969, and today we cannot assume that the jurist thought develops with the same quantity and quality as with the development of the information technologies. This should not represent a discouragement, but a motive plus for allowing the conditions for a dignified development of the cyber space starting with the internet as an acknowledged digital

[27] https://www.loc.gov/law/help/guide/nations/japan.php
[28] Jeff Kosseff, Cybersecurity Law, pg.356-357 (2017)

common sense on a minimum standard in all member States of UN. Then, we can discuss about the start of the Cyber revolution introduction, which although elaborated and debated from before[29], still has not happened.

The relation of the States toward the benefits of the cyber place speaks that they are still fighting with their own demons that pop up as a nus product from the wrong attachment and clinging to state sovereignty, and for the situation to become even more tragi-comedic, in this case, sovereignty does not exist, but the regulators around the world try to impose it. That is another reason why the Cyber revolution has not happened.

It would be ungrateful to come to the wrong conclusion that nothing has been done till now, contrary, the states have become more aware of the cyber space importance who can become even a threat for the national security and sovereignty. This is the second paradox of Cyber Law, since it is true that cyber space is not owned by any state, therefore sovereignty cannot exist in it, but at the same time we are aware of the existence of cyber-attacks that target directly the sovereignty of states, their whole election system, or leak millions of private information of citizens and similar. If the attributability can be attached to a given state, then the same it can be accused for the damage that aroused from the international wrongful cyber- attack.

The present momentum has grown for implementing international self-regulated norms of cyber space, which states will start to respect, recognize and guarantee them.

The confession towards our own self, that regardless of all the efforts in guarantying human rights in cyber place, has not happened. Everyday news are filled with articles for cyber-criminal that establishes a completely unjust allocation of big sum of financial money, and all of that conducted in a virtual way. The question that we are obliged to ask oneself is how to answer and approach to this unfairness that happens with the realization of the digital criminal intentions, whilst the digitalization of the criminal responsibility goes a little bit harder than expected? Maybe the time has come for digitalization of the international human rights to happen; acting like a stabilization code in the cyber space, as a tool for deterrence of human behavior that is focused on abuse of science's benefits?

[29] https://www.google.com/search?q=cyber+revolution&oq=cyber+revolution&aqs=chrome.0.0l6.3658j0j7&sourceid=chrome&ie=UTF-8

The future, is nothing but a product of the reality that we are practicing. In that case, the cyber human will be able to build the new cyber world, regarding the other people rights to decide their own 'digital assimilation' or the conduction of it on a self-regulated style. To be able to elaborate the foundation of the cyber humanity, we need to take a proper attitude toward its main material source- the Internet. Only, when the States are going to behave in 'bona fides' toward this common and effective realization in their respective territories, then we can speak about the start of the process of mankind digitalization and the creation of the cyber human. For the transformation process to happen, people must primarily use and learn a proper cyber alphabetization, becoming aware of the possible outcomes from the internet; just as we use: water, air, stars, that's existing for everyone. After the digital awakening of humanity, depending on the complexity of the digital alphabetization, the digital assimilation will follow, and the existence of resistance shall also take part, but the self-regulated concept will prevail, and people will voluntarily approach, demanding even the cyber assimilation. Like that, the stable digital communities, then societies, afterwards countries will create and establish a self-regulated digital world on which undigitalized people can accede in anytime in accordance with their needs and self-regulation.

If, States decide to fully acknowledge, respect, protect and guarantee this constitutive legal principle of digital commons, then they will need firstly to agree on the share of the present cyber benefits with all mankind and then taking the steps toward the mutual foundation of the digital world.

The basic reason for State existence is to secure the health and life of its citizens, thus human rights violation in the cyber place cannot stay without a proper sanction in the real world. Breaches of privacy, secrecy of letters, to bigger violations of human individuality are adding up to the frequency of the existent social frustration that causes damage to the trinity of dignity- autonomy- freedom of human beings and with it disturbing the balance of mankind in objective sense, through visualization of the digital criminal intention translated in real world.

The approach to criminogenic behavior or criminal deeds must always be the same, but in the process of settling the punishment, a maximum individualization and humanization of same must accomplish the punishments, regardless of the type of criminal behavior. Equality in this approach, in sense of absolute respect towards the

legal institution that is attacked with the attack of the protected subject from the legal order and the obligatory 'restitution in integrum' for the unlawful acquired property.

III.2

The digitalization of human rights would mean digitalization of the idea of human rights in cyber space as an answer to the evil that is present from the beginning of mankind history and it will continue to exist in the cyber space also. Digitalization would lead to visualization of the customary international human rights law i.e. the Universal Declaration for Human Rights in the digital world, or in other words that would found a replication of the duty for promotion of human rights into an international self-regulated regime for respecting human rights in cyber space from all cyber entities as guide for self-control toolkit of cyber space.

The digitalization would mean creating a 'lex mercartoria' of cyber space, and its users will start to incorporate in their cyber consciousness the set of international human rights, if they have not done this till now, which- maybe is the reason why they have persuaded themselves on criminal behavior toward other beings of our own kind. Lex mercartoria was initially created to codify and systematize the trading customs of merchants in order to ease the communication and trading process in whole. In Cyber Law that would mean creating an international regime which will set up the grounds for self-regulated model of access to human rights as a concept for digital respect i.e. digitalization of human rights.

Jurists around the globe[30] have not stayed blind in front of the fact that the benefits from the information technology did not just contributed to the development and establishment of a completely new law discipline, but also in generating human rights. At the same time, the first paradox of Cyber Law appears as cyberplace presents an arena of improvement and violation of human rights at the same time. The negative side and the danger of human rights abuse shows up as a consequence of the abuse of the benefits from the information technology, that is why it is necessary to respond with reciprocity, by digitalizing human rights as a counter measure in the space that sometimes allows their violation. The reflection of the objective reality of human rights in the cyber space will also mean an instant legal alphabetical of citizens around the globe and uplift of the

[30] Claudia Padovani, Andrew Calabrese (eds.), Communication Rights and Social Justice, Global Transformations in Media and Communication Research (2014)

collective consciousness, its upgrade and focus on other subjects from the benefits of Science, Arts, cultural mutual international life and order.

III.3.

The international regime must take into consideration the weaknesses and failures of the past, the possible obstacles in the future and to have into account the never-ending progress of Science and Art. The spirit of the same should announce not just the Cyber revolution, but the progress of Science and Art as one. Obligatory would be the acknowledgment of the present development of individual rights and freedoms and their shift in the digital consciousness of cyber space. Limiting the self-regulation in manner of respecting and not harming human rights, the international regime must allow the respect of human dignity- reason- autonomy while harvesting the benefits of the digital commons.

But in Cyber Law, we must allow ourselves to analyze things from a different perspective. That is why in addition to this research are the draft cyber articles, with hope that they will catalyze the Cyber revolution and present a deterrence toolkit by itself for deterring people from criminal or any kind of abuse of the digital commons. On first look it seems like the digitalization will implement a minimum standard of promotion of international human rights, but inside its articles the awakening of mankind consciousness is in front of the reader eyes.

The draft cyber articles are a product of the Internet existence, inspired from the Outer Space Treaty and the Universal Declaration for Human Rights, or it can be assumed that they provide detail elaboration of article 28 of the Universal Declaration for Human Rights. The cyber articles are crystalizing the commons that have created because of the benefits of Science and Art, accenting the need for cyber self-regulation. The first part of the draft articles is reserved for the legal principles (art.1-art. 4), the second part is reserved for State obligations and duties (art. 4- art.9) and the last part (art. 10- art. 11) elaborates the digitalization of Human Rights.

APPENDIX

- **THE DRAFT CYBER ARTICLES ON DIGITALIZATION OF HUMAN RIGHTS-**

Narrative

Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world and cyber place, the State Parties to this Treaty, inspired by the great prospects opening up before mankind as a result of the progress of Science and Arts,

Re affirming the right to freely participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits and the right to protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author,

Recognizing the information technologies era and its fast development,

Inspired by the great prospects opening before mankind as a result of the progress of Science and Art,

Respecting their autonomy and welcoming its progress for the benefit of all peoples irrespective of the degree of their State economic or scientific development,

Recognizing the common interest of all mankind in the progress of Science and Arts for peaceful purposes,

Believing in the commons and self-regulation concept of the Internet, that can lead to the establishment of perpetual equality,

Wishing to implement the commons concept on all other scientific discoveries who like the Internet can fall under this concept

Desiring to contribute to broad international cooperation in the scientific and artistic investigation,

Believing that such cooperation will contribute to the development of mutual understanding and to the strengthening of friendly relations between States and peoples,

Confirming its determination to abolish and rehabilitate all forms of criminogenic behavior regardless if it's in the real or virtual world,

Recalling the "Budapest Convention on Cybercrime", which was adopted by the Council of Europe, adopted on 23 November 2001,

Recalling the "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space", which was adopted unanimously by the United Nations General Assembly on 13 December 1963

Accepting the reality of creation of new generations of human rights, because of the respective progress of Sciences and Arts,

Convinced that the Draft cyber-articles will further the purposes and principles of the Charter of the United Nations,

Have agreed on the following:

Article I

The legal principles governing the activities of states in the exploration and use of outer space shall be applicable in the enjoyment of the benefits from the progress of Science and Art.

The progress of Science and Art shall be carried for the interest and benefits of all people irrespective of their state economic or scientific development at the same time protecting the intellectual property rights of the inventor.

There shall be no discrimination of any kind in the free access to the benefits of Science and Art, and States shall facilitate and encourage international cooperation in such actions.

The freedom of scientific investigation and autonomy shall be guaranteed.

Article II

The Internet presents commons of mankind. As such, is not subject to national appropriation or restriction of use by any means.

When using the benefits from the Internet, one must not use it in a way to harm another.

The exploration and use of cyber space shall be conducted to improve the life standard of people, not to worsen it.

State Parties to the Treaty shall carry on activities in the Internet in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.

Article III

Behaviors on the Internet from any entity are guided by the principle of self-regulation.

Self-regulation presents the amount of capability that one State, non-governmental entity or person can control one's behavior.

Article IV

States while nurturing the benefits from Sciences and Arts will be guided from the principle of cooperation and mutual assistance and shall conduct all their activities with due regard to the corresponding interests of all other States Parties to the Treaty.

State Parties shall take appropriate measures to promote the international cooperation and understanding in cyber space.

Article V

States shall take appropriate measures to prepare its citizen to be cyber literate.

Article VI

State Parties to this Treaty shall take appropriate measures to secure and guarantee free access to and implementation of the benefits from the Information technology and other Sciences and Arts in the daily lives of its citizens.

Article VII

State Parties to this Treaty have duty toward the establishment of international and national cyber societies that have respect for human rights.

Article VIII

State Parties to this Treaty shall adopt the Budapest Convention on Cybercrime or present proofs for adequate legislative measures against cybercrime.

Article IX

State Parties to this Treaty oblige to digitalize the Universal Declaration of Human Rights on all languages that are spoken on its territory and manage its free continuous access to its citizen and in cyber space.

Support in this process can be given from the UN Depositary Library, or its branches.

Article X

State Parties to this Treaty acknowledge the existence of a new generation of human rights because of article 27 from the Universal Declaration for Human Rights, the right to freely participate in the cultural life of the community, to enjoy the arts and to share in scientific advancements and its benefits.

In that spirit, State Parties agree to approach to the establishment of Fourth Generation of International Human Rights.

State Parties declare the recognition of the possibilities that come with the establishment of new Human Rights that correspond with the social reality of the present time.

BIBLIOGRAPHY

Books:

- Гоце Наумовски, Дајан Роуланд, Јута Кол, Ендрју Чарлсворт, Право На Информатичка Технологија, Скопје, (2013)
- Ѓорѓи Манојловиќ, Методија Каневчев, Македонско Кривично Право општ дел седмо, изменето и дополнето издание, (2010)
- Lawrence Lessing, Codes and Other Laws of Cyberspace, 1999, New York Basic Books and version 2.0 (2006)
- Fabio Tronchetti, The exploitation of natural resources of the moon and other celestial bodies: a proposal for a legal regime, (2009)
- Jeff Kosseff, Cybersecurity Law, (2017)
- Claudia Padovani, Andrew Calabrese (eds.), Communication Rights and Social Justice, Global Transformations in Media and Communication Research, (2014)
- Chris Edwards, Nigel Savage, Information Technology& The Law, (1986)
- Zeinab Karake Shalhoub and Sheikha Lubna Al Qasimi, Cyber Law and Cyber Security in Developing and Emerging Economies, (2010)
- Diane, PhD. Rowland, Elizabeth MacDonald, Diane Rowland-Information Technology Law, (2000)
- J. M. Balkin & Jack Balkin & James Grimmelmann & Eddan Katz & Nimrod Kozlovski & Shlomit Wagman & Tal Zarsky, Cybercrime- Digital Cops In a Networked Environment, (2007)

Articles:

- Nouri Neshat, Saeid, Communication Rights: Fourth Generation of Human Rights, (2003)
- V. Mandl, Das Weltraum- Recht: Ein Problem der Raumfahrt (1932)
- B. Cheng, Space Objects and Their Various Connecting Factors, in Outlook on Space Law over the Next 20 Years (Eds. G. Lafferranderie & D. Crowther), pg. 203 (1997)
- Hans J. Kleinsteuber, Self-regulation, Co-regulation, State Regulation, The Internet between Regulation and Governance: https://www.osce.org/fom/13844?download=true

- Mary Ellen O'Connell, International Law: Meeting Summary, Cyber Security and International Law, Chatham House, 29 May 2012 : https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf

INTERNET:

- Macedonian dictionary: http://makedonski.info/show/маниja
- List of some cyber organizations: https://cybersecurityventures.com/cybersecurity-associations/
- Legislature of G-7: https://www.loc.gov/law/help/guide/federal.php https://www.legislation.gov.uk https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx http://laws.justice.gc.ca/eng/ https://www.loc.gov/law/help/guide/nations/japan.php
- Internet censorship and surveillance by country: https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country
- Half of all countries aware but lacking national plan on cybersecurity, UN agency reports: http://www.un.org/sustainabledevelopment/blog/2017/07/half-of-all-countries-aware-but-lacking-national-plan-on-cybersecurity-un-agency-reports/
- Who really sets global security standards: https://www.networkworld.com/article/2231519/security/who-really-sets-global-cybersecurity-standards-.html?page=2
- Cyber revolution: https://www.google.com/search?q=cyber+revolution&oq=cyber+revolution&aqs=chrome.0.0l6.3658j0j7&sourceid=chrome&ie=UTF-8
- Protecting the Internet as Common Heritage of Mankind, Malta's official statement:https://www.academia.edu/19974250/Protecting_the_Internet_as_Common_Heritage_of_Mankind