ISSN 2220 - 461X

Viti i XIII-të i Botimit, Nr.2, Dhjetor 2021

OPTIME

Revistë shkencore e "ALBANIAN UNIVERSITY"

TIRANË

OPTIME Viti i XIII-të i Botimit, Nr.2 ,Dhjetor 2021 Revistë shkencore e "ALBANIAN UNIVERSITY"

Bulevardi: "Zogu i I-*rë*", Tiranë, Shqipëri (Albania) ♦ Tel (+355) 4 2271602

optime@albanianuniversity.edu.al

ISSN 2220-461X

Shtëpia Botuese & Shtypshkronja "Albanian University Press".
Adresa: Bulevardi "Zogu I", Tiranë, Albania
Mobile: +355 (0) 699441011
e-mail: pressalbaniauniversity@gmail.com

ISSN 2220 - 461X

Viti i XIII-të i Botimit, Nr.2, Dhjetor 2021

OPTIME

SPECIAL ISSUE

JEAN MONNET MODULE

EUWEB

Tiranë 2021

ISSN: 2220-461X

SCIENTIFIC PUBLICATION "Albanian University"

Address: Bulevardi Zogu I. tel. +355 4 2271602 e-mail: optime@albanianuniversity.edu.al

PUBLISHING Albanian University Press. Address: Boulevard "Zogu i I", Tirana, Albania Mobile: +355 (0) 699441011
e-mail: pressalbaniauniversity@gmail.com, www.albanianuniversity.edu.al,

ISSN: 2220-461X

Botime Shkencore të "Albanian University"

Adresa: Bulevardi Zogu I. tel. +355 4 2271602 e-mail: optime@albanianuniversity.edu.al

Shtëpia Botuese Albanian University Press. Adresa: Bulevardi "Zogu i Pare", Tiranë, Albania
Mobile: +355 (0) 699441011
e-mail: pressalbaniauniversity@gmail.com, www.albanianuniversity.edu.al,

ESSAYS

YOUNG RESEARCHERS

STUDENT RESEARCH AND REPORT WRITING

PËRMBAJTJA

ARTIKUJ SHKENCORË TË KËRKUESVE TË RINJ

ARTIKUJ SHKENCORË TË STUDENTËVE

EU-WESTERN BALKANS COOPERATION ON JUSTICE AND HOME AFFAIRS

Second Edition

ESSAYS

edited by

Teresa Russo, Anna Oriolo, Gaspare Dalia

Editorial Assistants: Stefano Busillo and Emanuele Vannata

CYBERCRIME REGULATIONS: NEED FOR A NEW INTERNATIONAL APPROACH?

Natasa Doneva*

***University "Goce Delčev" of Štip (Republic of North Macedonia), Faculty of Law (natasa.doneva@ugd.edu.mk)**

Abstract

Cybercrimes, cyber terrorism and cyber war are the pandemic of the 21st century. This problem existed before, but lately they have spread with a rapid speed, and have modified from their basic appearance, which makes them difficult to follow. The purpose of this paper is to show the need for a cyber convention of a new kind, and to explain the need for better international legal framework. The paper is "dealing "first with the European Convention of Cybercrime and its use. Also having in mind that the cyber field is not only consisted from cybercrimes/ offences but also with cyber terrorism and cyber wars, the second part of the paper is dedicated to the need of a new Digital convention. The last part is giving a brief overlook of the Macedonian legislation considering the cybercrimes.

Keywords: *Conventions, Cybercrimes, International Courts, Tallinn Manual*.

RREGULLORET E KRIMIT KIBERNETIK: NEVOJË PËR NJË QASJE TË RE NDËRKOMBËTARE?

Natasa Doneva[*]

[*]**Universiteti "Goce Delčev" i Štip (Republika e Maqedonisë së Veriut), Fakulteti i Drejtësisë (natasa.doneva@ugd.edu.mk)**

Abstrakt

Krimet kibernetike, terrorizmi kibernetik dhe lufta kibernetike janë pandemia e shekullit 21. Ky problem ekzistonte përpara, por kohët e fundit ato janë shpërndarë me një shpejtësi marramendëse dhe kanë modifikuar pamjen e tyre fillestare, gjë që i bën më të vështirë për t'i ndjekur. Qëllimi i këtij punimi është të tregojë nevojën për një konventë kibernetike të llojit të ri dhe të shpjegojë nevojën për një kuadër ligjor ndërkombëtar më të mirë. Punimi "trajton" si fillim Konventën Evropiane të Krimit Kibernetik dhe përdorimin e saj. Gjithashtu, duke patur në mendje se fusha kibernetike nuk konsiston vetëm në krimet/kudravajtjet kibernetike, por edhe në terrorizmin kibernetik dhe luftrat kibernetike, në pjesën e dytë punimi fokusohet në nevojën e një konvente të re digjitale. Pjesa e fundit përmban një panoramë të shkurtër të legjislacionit maqedonas lidhur me krimin kibernetik,

Fjalë kyçe: *konventat, krimi kibernetik, gjykatat ndërkombëtare, Manuali i Tallinn-it.*

1. Introduction

Cybercrime, cyber terrorism and cyber war, so far are still an enigma that has been studied by a different profile of experts. The tendency is to explain the more current cyber (information) war, the attitude of the world powers towards the new replacement for the conventional war, the preparation and formation of cyber centers by the states and the possible vision of a new army composed only of hackers armed with a single arsenal-the computer. Hence, it is inevitable to refer to the legal regulations that tries to deal with "cybermania" both nationally and internationally.

Lately, many more cybercrime activities are manifested and originated internationally than nationally. This only further indicates the weight and impact that this crime has worldwide.

From the huge constellation of international paperwork that refers precisely to the prevention and suppression of cybercrime, we will list a few, which are adopted by international organizations or at the initiative of some countries. There are a number of regional as well as international organizations that have already adopted documents related to cybercrime / security (1).

Among others, we would mention the following:

- The Council of Europe Convention on Cybercrime (2001) (2);
- The Shanghai Cooperation Organisation (SCO) – Shanghai Convention on Combatting Terrorism, Separatism and Extremism (2001) (3);

- The OECD Policy Guidance on Online Identity Theft (2008) (4);
- The Shanghai Cooperation Organisation (SCO) – Cooperation in the Field of Information Security (2008) (5);
- The League of Arab States Convention on Combating Information Technology Offences (2010) (6);
- HIPCAR – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (2012) (7);
- The European Union Directive on attacks against information systems (2013) (8);
- UNODC Expert Group comprehensive study on cybercrime (9);

African Union African Union Convention on Cyber Security and Personal Data Protection (2014) (10);

- The Commonwealth - Report of the Working Group of Experts on Cybercrime (2014) (11).

Primarily, the intention of these international treaties and conventions should be to help unify the legislations of different countries. Cybercrime and cyber terrorism as global problems are the same for all countries, with the same consequences for all economies, with the same repercussions for all individuals. Then why so many different regulations for the same issue? These criminal activities are gaining momentum across a number of countries, they are gaining international recognition and, as such, are seeking an international response. The most ideal solution is the cooperation of the states together. This means first ratification of the international conventions related to this matter, incrimination in the national legislation of the new crimes in the field of cybercrime, mutual assistance in the detection, suppression and prevention of this high-tech crime.
The specificity of this issue requires its elaboration at a higher level than the national one. Hierarchically there are the bilateral agreements, with which two countries regulate their relations for a certain issue. Afterwards, a step higher, multilateral agreements with which several countries are obliged to adhere to the rules and norms to which they have previously agreed. Regional agreements also offer their advantages and benefits, but none of these are enough to follow the "dark path" paved by the rapid rise of cybercrime. That is why there is a need for greater "intervention" of a greater force. So far this kind of legal, international protection is offered by the European Cybercrime Convention (also known as Budapest Convention) adopted in 2001 (12), which obliges the Council of Europe Member States and other non-Council Member States who participate in its drafting.
The European Convention on Cybercrime emphasizes the need for detailed regulation of computer crimes, that already have an international character. They are spreading with incredible speed, which “infects” all countries, without exception. Due to the transnational character, a special joint international cooperation is needed between the states and their bodies for effective action, prevention and detection of cybercrime.
The Convention consists of a preamble and four chapters:

1. use / explanation of terms;
2. substantive and procedural law;
3. international cooperation;
4. final provisions.

Certainly, Chapters II and III are the most fruitful in terms of computer incrimination of crimes. Starting with article 2, the Convention provides provisions for unauthorized access, unauthorized interception, intrusion (interference) in data, intrusion (interference) in the system, misuse of a device, computer-related forgery, computer-related fraud, acts related to child pornography, as well as works related to copyright and other related rights. This Convention regulates the effort and assistance, as well as the responsibility of legal entities. It is interesting that the Convention also pays attention to the need for expeditious saving of stored computer data, secrecy and caution in their storage, search or seizure.
Article 35 of the Convention is interesting. It requires each signatory to designate a point of contact that will be made available 24 hours / 7 days a week, in order to carry out investigative and other procedural actions in relation to computer system and data-related crimes, gathering evidence in electronic form or simple simplified 24/7 network adaptation.
Also, the signatory states of the Convention should pay special attention to the way of collecting data because they should respect the basic human rights and freedoms, proclaimed in a number of international documents, such as the Universal Declaration of Human Rights and Freedoms (1948), the European Convention for Human Rights (1950), the International Covenant on Civil and Political Rights (1966).

2. The Need of New "Geneva" Convention?

The adoption of the Budapest Convention certainly has a number of benefits. It points to the alarm and awareness of the world public of the danger lurking in the crimes of the new age. It exposes the desire to cover as many aspects as possible in the precise legal regulation and placement of this crime in a well-established legal framework. However, it also has some shortcomings. Thus, it is not specified in detail how and with the use of which methods, the states should deal with this crime. The list that initially covers these crimes, must not be deemed definitive. On the contrary, it should always be open to the introduction, incrimination of new computer crimes, because they appear in a new form every day. Plus we must have in mind the danger of their modification. They change the form of manifestation or the manner of execution.
The Convention, it may be well established by content, but still is binding only on the member States of the Council of Europe and those who have participated in its preparation. But what about the other numerous countries where cybercrime is present - or rather said all other countries - because this crime is present in literally every country on the planet. So that is why, the need for the adoption / drafting of a universal Convention on Cybercrime on a international, global nature still exists. There is still a need to eliminate the "legal gap" in incriminating this crime in the same way in different countries, to establish the same methods in preventing these crimes and their recognition in another country (for example, it often happens that the state that seeks assistance for cybercrime from another country, does not recognize and does not allow the legality of gathering evidence. Or perhaps it may disagree with the stages of detection of this crime and the way in which the requesting state works).
In this context I would mention several profiles of firms and experts that insist on a new digital convention. For example*:* "[i]n February this year, Microsoft President and Chief Legal Officer Brad Smith took the stage at the RSA security conference in San Francisco to make the case for a 'Digital Geneva Convention' that protects civilians from state-

sponsored cyber-attacks. Given that main intent of the last Geneva Convention (1949) was to protect civilians and non-combatants during warfare, this call to action – a Geneva 5.0 – is both timely and welcome" (13).

According to Microsoft, the purpose of this Convention would be to "commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust" (14). The propose of this kind of a convention, consists of a series of principles like: exercise restraint in developing cyber weapons; no targeting of tech companies, private sector, or critical infrastructure; to assist private sector efforts to detect, contain, respond to, and recover in the face of cyberattacks; to agree to a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities; to agree to limit proliferation of cyber weapons; to limit engagement in cyber offensive operations. "Microsoft has also called for the establishment of an independent organization to investigate and attribute state responsibility for attacks, similar to the International Atomic Energy Agency, with technical experts from relevant stakeholder groups" (15).

This is one way of how this new convention can be seen. But also, it can be a little bit different. Here are some suggestions of how this convention can be made, and what sort of new courts should and could be established.

Given the current alarming situation, the rapid rise of digital crime (here we would mention cybercrime, cyber terrorism and cyber-information warfare) and the future prognoses of its escalation, it is more than obvious the need of an international convention that will comprehensively regulate cyber matter. A Convention that would detail the rules for detecting, prosecuting and punishing cybercrime, that would implement incriminations for crimes that will be the same for all countries in the world, and not just for a certain region (not to allow small localization, but globalization of conventions that will be ratified anywhere in the world or even better-provide provisions that would have erga omnes effect and jus cogens norms). Of course, the convention would offer more general provisions, and it would be up to the states to find a way to implement those provisions in their domestic regulative. This thesis may seem strange, utopian, too ambitious, but still correct and achievable. Because the nature of virtual, digital crime requires such an approach. The transnational action of these crimes is a parameter that is very important and can have different effects. Thus, if left as before, cybercrime may not be properly punished because different countries criminalize and punish it differently. In some cases, certain crimes are not provided as crimes in a law-framework, or the punishments are not the same. And all this facilitate the environment in which criminals are free from the bonds of justice. But if there are the same-kind of incriminations and similar sanctions and there is an international cooperation, these problems would not exist and we would no longer be afraid of anonymous people who can steal our identity, hackers who are ruthless soldiers, cyber abuse that is a draconian general and announces terrible wars.

Our position on this issue, was partly created due to the "evasion" of the 2001 European Convention on Cybercrime. Although it is formal, theoretically well thought out, its real

implementation and application is still missing. Primarily designed to operate on European soil, (*this Convention is open for signature to all Council of Europe member states, as well as to other non-Council of Europe countries that have participated in its drafting, but there is a mechanism, and it is a country that is not a member of the Council of Europe, nor has participated in the drafting of the Convention, but at the invitation of the Council and with the prior consent of the member states, to be able to accede to the Convention*) does not show enviable results in the fight against digital crime. The reasons for (failure) may be numerous, of different nature, but all together only once again show that there is an enormous need for a new global convention that will fully regulate the cyber "issues", and will be "mandatory literature" for all countries in the world, without exception.

Closest to our position on regulating and protecting against "cybermania" is the idea of introducing the so called Digital Geneva Convention. What does that mean and why exactly that name? The Digital Geneva Convention would be a digital copy of the famous Geneva Conventions (16) which are synonymous with the humanitarian law in the world. Namely, as a reminder, the first Geneva Convention protects the wounded and sick during armed conflicts, the second Geneva Convention protects the wounded at sea, the third Geneva Convention protects prisoners of war and introduces the rules for their conduct while the fourth Geneva Convention protects civilian populations, especially those in the occupied war zones. In fact, these Geneva Conventions are at the heart of international humanitarian law. The idea for the digital version of the Geneva Conventions once again further shows that the whole world fears cybercrime, cyber-attacks and cyber war. It means that the digital "fights" of the countries are no longer a joke or science fiction, on the contrary, they are a reality that is supported by the existence of cyber centers where "new soldiers" are trained. Therefore, the need for a Convention that will introduce international principles, rules, international tribunals to punish cybercriminals is more than a necessity.

Thus, the Digital Geneva Convention would protect citizens online in peacetime. It would greatly contribute to the efforts to make the Internet a safer place and to maintain confidence in the good side of technology. The nature of military conflicts has already changed, cyberspace is already rushing to rise to the first place in the war zones (besides war on land, sea, air ...). The world has already witnessed Stuxnet (17), Petya (18), WannaCry (19) attacks, and we can make the conclusion that cyberspace is a territory without laws, a territory without justice... and obviously the existing solutions for combating cybercrime did not live up to high expectations.

Our interest is especially focused in establishing an international court or cyber tribunal. To many, this seems very strange, perhaps illusory, because so far tribunals have been set up only for crimes against humanity, war crimes and crimes against peace. But these tribunals did not emerge until the end of the World War II, after the revelation of the Holocaust. So the question arise, should we wait for a cyber war to break out first, and only then to try to repair the unimaginable damage and start considering the opening of international tribunals for this kind of crimes? Why not prevent it while we can? The current cybercrime proceedings are conducted before courts that decide on "old" crimes. In most countries, there are usually no specialized courts with specialized staff to decide, rule on, or convict cybercrime. And this matter requires exactly that - specialization for work in the field of "cybermania". Thus, within the domestic legislation, it is desirable to have special court instances that would work exclusively with this *materia*. While on the

international stage, there is a need for international courts that will deal exclusively with cyber/digital crime, and as a basic "tool" they would have the eventual Convention on Cybercrime or Digital Convention. Or to paraphrase former U.S. prosecutor Attorney Benjamin B. Ferencz "there can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstance" (20).

A solution for the possible establishment of an international tribunal intended only for cybercrime, which will be based on fair principles, and will also provide mechanisms for the protection of human rights and freedoms. These established now, if realized, may be a historic step taken to detect, prevent and reverse the far-reaching consequences of cybercrime/cyberterrorism.

In the context of international cybercrime tribunals and an appropriate new convention on this issue, Norwegian judge Stein Schjolberg (21) has some very interesting views, believing that without an international court to "deal" with cybercrime, many cyber-attacks will go unpunished. In his recommendation – Recommendations for Potential New Global Legal Mechanisms Against Global Cyberattacks and Other Global Cybercrimes (22) – he talks about the need for an international tribunal, the reasons why the 2001 Cybercrime Convention did not "come to life" outside Europe, for the (not) appropriate terminology, but also he writes about the new cybercrimes that are a product of the new millennium (meaning they exist after 2001 and are not covered by the previous Convention on Cybercrime) and are improperly regulated. This judge has accomplished significant achievements in the field of cybercrime (23) and has published a huge number of papers.

3. Tallinn Manuals

The fast rise and the international cross-bordering of cybercrimes, have alarmed the urgent need of new international approaches. In 2013 the world heard about something called Tallinn Manual 1.0. And a few years later, Tallin Manual 2.0 was released. As Goldsmith and Loomis try to point out the difference between them, they explain "[t]he first version, Tallinn Manual 1.0, published in 2013, proposed to describe international law on cyber operations involving the use of force and in armed conflict more generally. Tallinn Manual 2.0, published in 2017, builds on and supersedes the original. It covers peacetime cyber operations as well as ones related to armed conflict, and it revises some of its earlier rules" (24).

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations provides 154 black letter rules detailing how international law applies to cyber operations during peacetime (25). As Jensen writes (26), both Tallinn Manuals were written by groups of international legal experts. The Tallin 2.0 included experts in human rights, space law, international telecommunications law). Also, members of the International Committee of the Red Cross were invited in the process (27). The "eternal dilemma" remains: can and should international law be applicable in the cyber sphere? If so, how and in which parts can international norms be mandatory for this kind of crime? So many questions arise and only few solutions to offer-in this way we can describe the current situation in this field!

4. Cyber Legal Framework in Macedonia

The Republic of Macedonia compared to other countries has a modest experience in the field of cybercrime and even more modest in terms of cyber security. In the archive of these crimes, which involve Macedonia, we can point out several cases of attacks on the websites of state institutions, disclosure of classified information and protection of personal data. Thus, in 2007, an analyst employed by the UBK (Security and Counterintelligence Directorate) stole secret documents from the digital archive and submitted them to a foreign country. However, the Ministry of Interior has never officially confirmed this case. In 2014, in Operation Spy (28), current and former members of the security sector were convicted of leaking classified information to foreign countries.
And when hacking websites is mentioned, there was a suspicious attack on the website of the President of the Republic of Macedonia (29), the Ministry of Transport and Communications, the Municipality of Veles (30) and several private portals (31) (32) (33). Although not all of the attacks cause material damage, they are still specific because they were the first to be attacked "digitally" in the country, and pointed out the major shortcomings that the security segments should have regulated. Given the fact that R. Macedonia signed the European Convention on Cybercrime in 2003, ratified it in 2004 (34) and entered into force in 2005, it is normal that it was infiltrated in the domestic legislation. It has found embodiment and application through a number of domestic regulations. Thus, the domestic legal framework for cybercrime is composed of several laws:

- Criminal Code (35);
- Law on Criminal Procedure (36);
- Law on Electronic Communications (37);
- Law on Interception of Communications (38);
- Law on Electronic Commerce (39);
- Law on Electronic Management (40);
- Law on Civil Procedure (41);
- Law on Electronic Data and Electronic Signature (42);
- Declaration for safer internet (43).

In the Macedonian legislation, the norms governing this matter, have been incorporated into existing laws, but still provided full incorporation of the Convention on Cybercrime. This move gave hope that Macedonia will deal much better and more efficiently with the challenge of cybercrime, that is rapidly changing and fluctuating, manifesting new forms every day.
In this context is the National Cyber Security Strategy 2018-2022 action plan (44) that was released in 2018. The purpose of this document is to define the steps in the implementation of the first National Cyber Security Strategy of the Republic of Macedonia 2018-2022. After the analysis of the cyber security capacities at the national level, a working group responsible for the development of strategic documents in the field of cyber security, was developed. It includes representatives of the three competent ministries for cyber security in the Republic of Macedonia - Ministry of Information Society and Administration, Ministry of Defense and Ministry of Interior.

There are three priority activities. One of the priority activities was the Establishment of the National Council for Cyber Security (45). The second one is forming a body with cyber operational capabilities security as a newly established independent body (agency, directorate) or as a newly formed organizational unit, i.e. body within existing authority. It's beginning was planned in 2019. And the third one was the preparation of a study for the identification of KII and VIS.
With this Strategy a few goals were set:

- cyber resistance;
- cyber capacity and culture for cyber security;
- dealing with cybercrime;
- cyber defense;
- cooperation and exchange of information.

The Macedonian legal framework considering cyber issues is still very "poor". The efforts that the country is making, especially in the implementation of the Convention in the domestic legislation, is on good level. But beside that fact, something is missing. The number of cybercrimes in the country is increasing.

5. The Budapest Convention on Cybercrime: Comprehensive House Rules or Need for New Rulings?

Many authors are already talking about cyber law-internet law. And it can be defined like this: "[c]yber Law or IT Law is referred to as the Law of the Internet. The Cyber law definition says it is a legal system designed to deal with the Internet, computing, Cyberspace, and related legal issues. The apt introduction to Cyber Law is: It is 'paper laws' in the 'paperless world'" (46).
In addition to cybercrime, fears of catastrophic war are spreading at an alarming rate in the digital world. But not a classic, conventional war, but a far more terrifying cyber-information/information war. This fear is justified by the fact that, although there are no classic soldiers on the front here, there are hacker geniuses behind the computer, which alone can cause far more consequences than an entire army. Although there are no conventional weapons or bombs, there is a single mechanism – a computer. A device that can replace an entire arsenal of weapons and make far-reaching repercussions. The views of many experts in this field are divided. Some predict the start of this war in the very near future, some already locate its beginning. There are dozens of examples that show "symptoms" and variations of information technology – cyber war. And not to mention the numerous cases of cyber-attacks.
For example, we will mention here some of the most exposed cyber-attacks so far. Most of these attacks occurred after 2001, after the Budapest Convention was released. So, there is a room for discussing the "absence" of the convention concerning this situation.
Stuxnet is a malicious computer worm discovered in 2010, presumed to have been developed since 2005, with a primary purpose and target – Iran's nuclear program. Several media reports suggest that Staxnet (47) was intended to sabotage the Natanz uranium enrichment facility. The damage done to Nantanz could not initially point to the real problem until help was sought from experts who detected the Stuxnet virus in Iran's nuclear network.

Operation BugDrop is a cyber-attack that aims to penetrate critical infrastructure, media and scientific research. The intention is to collect sensitive information from the "targets" including recorded conversations, screenshots, documents, passwords. Most of the targets are located in Ukraine (48) and Russia, a smaller number in Austria and Saudi Arabia. The targets of this operation are primarily oil and gas companies; international organizations that monitor human rights, terrorism and cyber-attacks; engineering companies that design power plants, gas distribution, water supply; scientific research centers. The operation infects the victims through the so-called phishing attack.

Red October (49) is a malicious cyber espionage program discovered in October 2012, but it is assumed that it has successfully performed its task unnoticed for several years. The purpose of the operation was to record diplomatic secrets and even personal information, which was obtained from all devices, including mobile phones.

Guardian of Peace is the pseudonym under which a group of hackers published a series of protected data from the famous film studio Sony pictures. The hacked information included information about employees, their families, emails, copies of unreleased Sony movies. The hacker group asked the company not to play "The Interview" (50) a comedy film about the assassination of the North Korean leader. This request was taken very seriously because the threats referred to a terrorist attack in the cinemas where the film would eventually be shown (51). Sony has canceled the premiere of this movie and allowed only its download. Although many have linked the hacker group to North Korea, it has completely denied any involvement in the cyber-attack (52). Some theories point to a Sony insider or even go further accusing of a marketing campaign just to promote "The Interview". But the cyber-attack still has sparked a series of political escalations between the United States and North Korea (53).

Shamoon (also known as W32.DisTrack) (54) is a computer virus discovered in 2012. It deviates from the "classic" behavior of other viruses due to its destructive nature, time and cost required to recover a damaged and attacked computer. The virus spreads very quickly, occupying the entire system and stealing specific information that it gives to attackers, and then deletes them. The virus has attacked Saudi Arabia's national oil companies, Saudi Aramco and Qatar's RasGAs.

TV5 Monde is a global television network, which in 2015 was the victim of a cyber-attack (55), carried out by a hacker group known as CyberCaliphate. They managed to penetrate the internal systems, thus taking them completely for three hours. Even the next day TV5 Monde did not manage to completely take matters back into their own hands. The Facebook and Twitter networks of the television were also hacked. For the French authorities, the cyber-attack was an attack on freedom of expression and freedom of information.

And what would computer crime and information warfare (56) be without the accompanying component that rounds off the dark side of the digital age – cyber terrorism. We have heard, witnessed terrorism, we can debate its beginnings, its targets and victims, but are we competent to discuss virtual terrorism? Maybe the goals, the ideology of terrorism remain the same, but they definitely got a new direction in the way of acting, spreading the ideology, recruiting members. Terrorism and war are gaining new momentum, far more than we can imagine.

Evan though we already have the Budapest Convention on Cybercrime (and we can't deny the benefits from it), we have to be real about the situation: *rules versus praxis of*

the convention. And we need to be aware for Cybercrime regulations: the need for new housekeeping rules!
In this context the Internet Organised Crime Threat Assessment (IOCTA) should be mentioned. *Each year, Europol's European Cybercrime Centre (EC3) publishes the Internet Organised Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime – threats that impact governments, businesses and citizens in the EU* (57). In the next footnote, reference for all the IOCTA reports can be found, including the latest one from 2020 (58). For example, in the latest report there are pieces of information about cross-cutting crime facilitators and challenges to criminal investigations; cyber-dependent crime; child sexual exploitation online; payment fraud; criminal abuse of the Darkweb.

6. Conclusion

At the time of writing this paper, there is a possibility that new malwares, undercover information platforms, computer *sui generis* viruses, fortified spyware, and immunocompromised information weapons are being invented. The world is still having a hard time dealing with the current, detected and confirmed information crimes, and new ones are already in sight.
This paper is an attempt to delve deeper into the *materia* that was unimaginable in the past. It is currently very "popular", but still insufficiently researched, and with a forecast that warns of further escalation. All this only indicating the fact that we are talking about a topic that will reach its zenith in near future. An issue that will become an increasing reality, with which countries risk being easy targets because in a short time anonymous hackers will be able to penetrate the core of the state security system and shape it as they wish, with a very low probability that someday their identity will be revealed. Thus, each country can become easy prey for another country, which has better information resources. In this way, the beginning of new wars is predicted, which instead of the conventional arsenals of weapons, will now have only a single computer, which is worth more than all the heavy artillery.
Therefore, there should be far more analysis for computer crimes, from the original forms of occurrence to today's new manifestations. In the meantime, the academy field and experts should address as much as possible to the legal regulations of states regarding this matter. Namely, not all countries deal with cybercrime equally. It has a different treatment in different countries. The presence of conventions, declarations and other international documents does not always have a drastic effect on the final concretization of all previous occurrences of computer crimes, nor on a unified fight against them. The need for new mechanisms with an international sign still exists.

References

(1) S. SCHJOLBERG, *The History of Cybercrime; Cybercrime Research Institute*, Cologne, 2017.
(2) Council of Europe's Convention on cybercrime, signed in Budapest on 23 November 2001, available at www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
(3) Shanghai Cooperation Organisation's Shanghai Convention on Combating Terrorism, Separatism and Extremism, 15 June 2001, available at www.refworld.org/pdfid/49f5d9f92.pdf.

(4) OECD Policy Guidance on Online Identity Theft, June 2008, www.oecd.org/sti/consumer/40879136.pdf.
(5) Shanghai Cooperation Organisation's Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, 16 June 2009, available at www.ccdcoe.org/organisations/sco/.
(6) League of Arab States' Arab Convention on Combating Information Technology Offences, 21 December 2012, available at www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.
(7) *Enhancing competitiveness in the Caribbean through the harmonization of ICT Policies, Legislation and Regulatory Procedures*, in *International Telecommunication Union*, available at www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx.
(8) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013, *on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*, in OJ L 218 of 14 August 2013, pp. 8-14.
(9) Sixth session of the Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, Vienna, 27-29 July 2020, available at www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2020.html.
(10) African Union's Convention on Cyber Security and Personal Data Protection, 27 June 2014, available at www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
(11) Commonwealth Secretariat, *Report of the Commonwealth Working Group of Experts on Cybercrime*, in *Commonwealth Law Bulletin*, Vol. 40, No. 3, 2014, pp. 502-561, available at www.tandfonline.com/doi/abs/10.1080/03050718.2014.937068.
(12) See the Budapest Convention and related standards, available at www.coe.int/en/web/cybercrime/the-budapest-convention.
(13) J. GUAY, L. RUDNICK, *What the Digital Geneva Convention Means for the Future of Humanitarian Action*, in *unhrc.org*, 25 June 2017, available at www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/.
(14) Access Now, *A Digital Rights Approach to the Tech Accord and the Digital Geneva Convention*, September 2018.
(15) More about this policy paper in Microsoft, *Establishing an International Cyberattack Attribution Organization to Strengthen Trust Online*. *Microsoft Policy Papers*, available at www.query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI.
(16) Geneva Conventions (I, II, III, IV) of 12 August 1949 and Additional Protocols (I, II) of 8 June 1977, available at www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm.
(17) Stuxnet is a malicious computer worm (discovered in 2010) but thought to have been in development since at least 2005.
(18) Petya is a family of encrypting malware that was first discovered in 2016.
(19) WannaCry ransomware attack was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
(20) Benjamin B. Ferencz is an American lawyer. He was an investigator of Nazi war crimes after World War II and the chief prosecutor for the United States Army at the Einsatzgruppen Trial.
(21) Stein Schjolberg is a Norwegian judge and international cybercrime expert. In 2007 he was appointed Chairman of the High-Level Experts Group (HLEG) on cybersecurity, which includes more than 100 experts from around the world.
(22) S. SCHJOLBERG, *An International Criminal Tribunal for Cyberspace (ICTC). Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes. A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group*, March 2012.
(23) S. SCHJOLBERG, *The History of Global Harmonization on Cybercrime Legislation-The Road to Geneva*, December 2008.
(24) J. GOLDSMITH, A. LOOMIS; *"Defend Forward" and Sovereignty*, in *Hoover Working Group on National Security, Technology and Law. Aegis Series Paper No. 2102*, 29 April 2021.
(25) P. COLIN, *Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations*, in *Washington International Law Journal*, No. 58, 2019, p. 581 ff.

(26) Eric Talboat Jensen was member of both International Groups of experts for Tallin Manual 1.0 & Tallin Manual 2.0.
(27) E.T. JENSEN, *The Tallinn Manual 2.0: Highlights and Insights*, in *Georgetown Journal of International Law*, Vol. 48, No. 3, 2017, pp. 735-778.
(28) For more information about this case see *Шпион*, in *akademik.mk*, 11 March 2014, available at https://akademik.mk/sudenje/shpion-2/.
(29) *Хакирана веб страницата на Претседателот*, in *mk.tv21.tv*, 27 February 2017, available at www.mk.tv21.tv/hakirana-veb-stranitsata-na-pretsedatelot/.
(30) Veles is a city in the central part of North Macedonia.
(31) A. TOMIC, *Анализа со Митрески: Сајбер напад од 35 милиони IP адреси е многу скап. Кој е мотивот?*, in *faktor.mk*, 24 July 2020, available at www.faktor.mk/analiza-so-mitreski-sajber-napad-od-35-milioni-ip-adresi-e-mnogu-skap-koj-e-motivot.
(32) K. OZIMEC, *Паднати веб-сајтовите на повеќе македонски медиуми - технички проблем или напад?*, in *Deutsche Welle*, 19 November 2016.
(33) *Сајбер нападите во предизборието може да имаат сериозни политички импликации*, in *focus.mk*, 6 February 2020, available at www.fokus.mk/ordanoski-sajber-napadite-vo-predizborieto-mozhe-da-imaat-seriozni-politichki-implikatsii/.
(34) Закон за ратификација на Конвенцијата за компјутерски криминал; available at www.rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41e.
(35) Кривичен законик, available at www.slvesnik.com.mk/Issues/90E0B29D702D49A48DBCC2239374B927.pdf.
(36) Закон за кривична постапка; Службен весник на РМ, бр.150 од 2010, available at www.jorm.gov.mk/wp-content/uploads/2016/03/Zakon_za_Krivicna_postapka_150_18112010-2.pdf.
(37) Available at www.mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/Zakon%20za%20elektronskite%20komunikacii.pdf.
(38) Закон за следење на комуникациите, available at www.mvr.gov.mk/Upload/Documents/Zakon%20za%20sledenje%20na%20komunikaciite.pdf.
(39) Закон за електронска трговија, available at https://www.pravdiko.mk/zakon-za-elektronska-trgovija/.
(40) Закон за електронско управување и електронски услуги, available at www.mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zakon_za_elektronsko_upravuvanje_i_elektronski_uslugi_0.pdf.
(41) Закон за парнична постапка.
(42) Available at www.mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zededu.pdf.
(43) Декларација за побезбеден интернет, www.dejure.mk/zakon/deklaracija-za-pobezbeden-internet.
(44) National Cyber Security Strategy, December 2018, available at www.mvr.gov.mk/Upload/Editor_Upload/AP%20v1_13MK.pdf.
(45) See decision to form this Council available at www.dejure.mk/zakon/odluka-za-formiranje-na-nacionalen-sovet-za-sajber-bezbednost.
(46) I. UPADHYAY, *Cyber Law: A Comprehensive Guide For 2021*, in *jigsawacademy*, 13 September 2020, available at www.jigsawacademy.com/blogs/cyber-security/what-is-cyber-law/.
(47) M. HOLLOWAY, *Stuxnet Worm Attack on Iranian Nuclear Facilities*, in *large.standfor.edu*, 16 July 2015, available at www.large.stanford.edu/courses/2015/ph241/holloway1/.
(48) P. PAGANINI, *Operation BugDrop – Hackers Siphoned 600GB Taking Control of PC Microphones*, in *securityaffairs*, 21 February 2017, available at www.securityaffairs.co/wordpress/56517/intelligence/operation-bugdrop-ukraine.html.
(49) Global Research & Analysis Team – Kaspersky Lab, "*Red October" Diplomatic Cyber Attacks Investigation*, in *securelist.com*, 14 January 2013, available at www.securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/.
(50) K. GROW, *Sony Cancels 'Interview' New York Premiere Amid Terror Threats,* in *RollingStones*, 17 December 2014, available at www.rollingstone.com/movies/movie-news/sony-cancels-interview-new-york-premiere-amid-terror-threats-194486/.
(51) D. McNARY*, Sony Has 'No Further Release Plans' for 'The Interview'*, in *variety.com*, 17 December 2014, available at www.variety.com/2014/film/news/sony-has-no-further-release-plans-for-the-interview-1201382167/.

(52) *Who are the Guardians of Peace? A New Hacker Group Is on the Loose*, in pandasecurity.com, 8 January 2015, available at www.pandasecurity.com/en/mediacenter/news/guardians-peace-new-hacker-group-loose/.
(53) *North Korea Berates Obama over The Interview Release*, in *BBC*, 27 December 2014, available at www.bbc.com/news/world-asia-30608179.
(54) E. SHEIN, *Incident Of The Week: Shamoon Virus Cripples Hundreds Of Computers*, in *CyberSecurityHub*, 14 December 2018, available at www.cshub.com/attacks/news/incident-of-the-week-shamoon-virus-cripples-hundreds-of-computers.
(55) *'Phishing email' the key to hacking of TV5Monde*, in *thelocal.fr*, 14 April 2015, available at www.thelocal.fr/20150414/how-the-french-channel-tv5-was-hacked/.
(56) M. HADJI-JANEV, M. BOGDANOSKI, *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*, 2015.
(57) Europol, *Internet Organised Crime Threat Assessment (IOCTA) - Strategic, Policy and Tactical Updates on the Fight Against Cybercrime*, available at www.europol.europa.eu/iocta-report.
(58) IOCTA reports, available at www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2.