The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law

Enver BUÇAJ[1]

Abstract: This paper scrutinizes and highlights imminent need to regulate cyber terrorism pheromone in line with principle of international law. In so doing, this paper intends to ascertain legal basis to regulate cyber terrorism at international level. It explains the normative conduct by drawing on adjustments of certain member states of European Union as well as from none-European member states. Particular attention will be given as to how Kosovo has addressed cyber terrorism within its legal framework of criminal acts. The paper also addresses practical consequences of cyber terrorism in context of cyber-attacks events in attempt to establish legal basis for its prevention and punishment of cyber criminals wherever it happens. The author articulates its arguments by examining the presumed threats as a result of cyber terrorism activities, as well as based on well-known cyber terrorist behaviors and constant literature that insinuate that cyber-attacks are imminent threats. Lastly, as there is neither a particular treaty nor State practices, the author considers of utmost importance to spell out different views and statistics alluding that the need to regulate cyber terrorism in line with principle of international criminal law is a necessity.

Keyword: Cyber Crime; Cyber Terrorism; International Criminal Law; Necessity

1. Introduction

Terrorism has become a permanent phenomenon of contemporary life, which contains a wide range of threats, including those against the security and welfare of ordinary people, against the stability of the state political system, economic development and the spread of democracy. Contemporary terrorists are more organized, more professionally well versed and better equipped than their predecessors have done throughout history. Technological development offers them new attack targets and "skill" technical updates (Department of Justice, 2001,

[1] Associate Professor, PhD, University of Prizren "Ukshin Hoti", Law Faculty, Kosovo, Address: 1 Shkronjat, Prizren 20000, Kosovo, Corresponding author: hazirifatos@gmail.com.

p. 51). Terrorists of tomorrow will be able to use the most modern equipment, chemical, biological or nuclear explosions to perform mass and political unrest.

Today's world is a society made up of diverse communication networks, where production and distribution of food, oil pipelines and gas and so forth, are not built by having in mind the idea that one day they will be exposed to risks terrorism. Already we have seen how both of these networks, civil air transport and mail delivery mechanisms turned against Americans on September 11, 2001 (Yonah, 2002, p. 6). Despite the maximum commitment of all parties that fight crime, whether national or international, must not have illusions and ideas that terrorism will be completely eradicated. Therefore, it is very important and necessary to determine the regulation of terrorism according to international criminal law principles.

Ben Saul noted that "a combination of pragmatic and principled arguments supports the case for the definition of terrorism in international law", including the need to punish violations of human rights, to protect the state's policy and to be very cautious, to distinguish public violence from domestic violence, and to ensure international peace and security (Saul, 2008, p. 1). On the other hand, Carlos Diaz-Paniagua, who has coordinated the negotiations of the United Nations Convention proposed comprehensive framework against international terrorism, has set out the need to provide a precise definition of terrorist activities in international law; starting from the knowledge that "criminal law has three goals: to declare that the conduct is prohibited, to prevent it and to express condemnation of society to acts of wrong" (Diaz, 2008). This brings to light that the role normative criminalization has special significance in the case of terrorism. Thus, international treaties on criminal law seek prevention and punishment of terrorist activity.

The definition of terrorism in international treaties and criminal law has multiple counts for several reasons:

• First and foremost, is that the definition of terrorism has symbolic and normative role to express the conviction of the people in society who commit prohibited acts.

• Second, it eases international agreements. A precise definition of terrorism obliges states to declare that they are willing to take stringent obligations on matters relating to the exercise of their national jurisdiction, also limits the scope of these obligations, makes less costly agreement etc.

• Thirdly, it gives a good basis for implementing mutual subjective legal obligations in judicial and police cooperation creates easier international. This function is particularly important in extradition where most legal systems require that terrorism be punishable as in the requesting state and the requested state.

• Fourth, help states to adopt national legislation to criminalize and punish terrorist acts defined in international treaties and in accordance with the obligations of their human rights.

The principle of *Nullum crimen nullum poena sine lege*s, requires states to determine exactly what actions are prohibited before anyone can be prosecuted or punished for committing these acts (Diaz, 2008, p. 46). However, research shows that lack a general agreement from the countries to define the term terrorism and this obviously is a major obstacle to reaching a consensus on this issue. If the legislation existed that would accept the term, the first definition would be essential because of righteousness, and it would not be necessary to left-sided definition and interpretation of states.

After all, many scholars on computer terrorism have noted that it is the moral obligation of all States to harmonize their legislation. Regarding the definition of terrorism, we share the same mindset, not because it is easy to agree blindly about an issue, but the logic complies with reality, which means that when a treatment gives no result, then it should activate other methods and in our opinion, harmonization of legislation is another appropriate and necessary step (FBI, 2010). Nevertheless, at present remains in doubt whether cyber security will run smoothly for organization such as NATO and other Internet users (Fidler, Pregent, &Vandurme, 2016).

2. Regulation of Terrorism Pursuant to Criminal Law in General and Computer Terrorism in International Acts

Despite the commitment of the international community, so far there is no general international instrument on combating terrorism. However, there are legal and normative acts that regulate this problem partly, and there is an obligation of every signatory state to adhere and respect them. It should be pointed out that so far there have been many problems on the drafting of international criminal law regulation

of computer terrorism and cybercrime.[1] Also, despite the obvious need for international cooperation regarding cybercrime, so far there is no genuine global multilateral instrument that would deal with this issue (FBI, 2010).

The issue of international cooperation in the fight against cybercrime was discussed at the Twelfth Congress of the United Nations, where it was discussed about crime prevention and criminal justice (Twlefth United Nation Congress on Prevention and Criminal Justice, 2010). Secretariat of the United Nations Office on Drugs and Crime (UNODC) in a working document prepared in anticipation of Congress has suggested, "the preparation of a comprehensive convention against cybercrime should be given special consideration"(Secretariat of UNODOC). Four regional preparatory meetings were held before Congress and, as stated in working document of UNODC in four these meetings have been calling for the drafting of an international convention to address cybercrime. Latin America and the Caribbean were strongly for such an idea, stressing "the necessity for the development of an international convention on cybercrime" (United Nations, 2010).

In addition, in its working document, UNODC notes that cybercrime at a high level is a transnational nature. Issues of national sovereignty of countries can hinder criminal investigations in the absence of active cooperation between law enforcement agencies of the jurisdictions involved. Also, the speed with which criminals computing can cause damage and can avoid detection puts law enforcement agencies under great pressure of time thus making international cooperation in this area even more compelling.

That is because many countries base on mutual legal assistance on the principle of double criminality, which requires that the act in question is punishable in both jurisdictions. Consequently, divergences in jurisdiction could harm the effective implementation. Where a jurisdiction lacks comprehensive legislation regarding cybercrime, or applies it in an insufficient way, then he could face a safe haven for

[1]Cybercrime was mentioned a lot in the news lately, ranging from phishing, botnets, hacking at ATM, share price manipulation, etc., and this is just to name a few of the many forms that can be online crime. Although it is difficult to quantify the actual development of cybercrime, an FBI source has revealed that the United States annual business losses for 2005 were only 67 billion dollars. In all cases, this figure has increased since that time. Reflecting the international open character of the Internet, cyber crime is a transnational phenomenon to a significant extent. Perpetrator and victim often will be placed under different jurisdictions, which represents an acute problem for law enforcement agencies regarding the conduct of the investigation and prosecution of crimes online.

cyber criminals. This kind of divergence can be treated only by joint efforts to harmonize legal standards and to improve cooperation between jurisdictions.

Currently, the main international conventions that addresses cybercrime is the Council of Europe Convention on Cybercrime, which was signed in Budapest in 2001 and entered into force in 2004. The Council of Europe, which is the European Union body was founded in 1949 to make the promotion of human rights, democracy and the rule of law in Europe now has 47 members, including 28 members of the European Union and Russia. By December 2009, 46 countries have signed the Convention on Cybercrime, while 26 of them have ratified (i.e. it was adopted in accordance with the internal constitutional requirements and thus proved to be applicable).[1]

Although the Convention was drafted under the auspices of the Council of Europe, it is open for signature by non-member countries. Four non-member countries participated in the negotiations on this treaty and signed it (the United States, Canada, Japan and South Africa), as well as a non-member country has ratified it (US). Therefore, we can say that this convention is not fully regional agreement and the fact that this convention has been ratified only one non-European country now suggests that this convention cannot be described as general convention.[2]

The Convention includes a number of crimes for which the signatory states are required to implement in their domestic law, including hacking, child pornography offenses and a number of works dealing with the violation of intellectual property. It also sets out a number of procedural mechanisms that signatories should be implemented in the country, including the granting of powers of law enforcement authorities to force Internet service provider to monitor the online activities. The convention calls upon the signatories to cooperate in a greater extent in the development of the investigation and prosecution of offenses concerning computer crime.

Practical application of Convention on Cybercrime suggests that "moving from legacy rules to cyber-specific principles is not adequate response in a number of ways, including that it does not change the reactive nature of the cyber threat approach or provide effective deterrence against state and non-state use of cyber technologies for various purposes" (Fidler, Pregent, & Vandurme, 2016, p. 16). It should be admitted that practice of this convention has many deficiencies due to

[1]COUNCIL, O.E. (2001). Convention on Cybercrime. Budapest, November, 53.
[2] Ibid, 54.

many other factors, however, precisely due to its immense nature to address cyber terrorism, cyber security remains high in the agenda of policy makers, and as a matter of law nationally and internationally. Thus, it is relevant for thinking about regulating it with principles of international criminal law.

Convention of Council of Europe on cybercrime is already in force for more than twelve years and has a wide range in all international agreements dealing with cybercrime. It is estimated that the signatories of convention includes a third of current Internet users, and its signing is open to countries which are not members of the Council of Europe where four non-European countries have already signed it.

Cybercrime affects not only in developed economies. There are more Internet users in developed countries than in underdeveloped countries and a study suggests that emerging economies may be particularly vulnerable to cybercrime. It is clear that effective combating cybercrime requires overall cooperation, including a significantly greater number of countries than the number of signatory countries of the Council of Europe Convention on cybercrime. Surely, such a thing will prove to be a challenge and return to the preparatory phase of drafting a general convention from scratch could involve years of diplomatic dispute, a battle that might be unsuccessful.

Given that existing convention has proved reasonably effective and that the signatory parties have gained valuable experience in its implementation, it seems futile to ignore. But the demand for the Convention of the Council of Europe to become a general standard as it is in current form seems likely to be less controversial considering the possibility that it may be seen as a blow to countries which did not say anything during its drafting. However, the European Council has agreed that the treaty could be updated and is now open for signature by non-member countries. The next Congress will probably provide the opportunity to suggest updating the Convention on Cybercrime, aiming at expanding the number of members.[1]It remains to be seen whether the Convention will gain greater recognition beyond the region and the continent of Europe. Even though the US is a signatory, we think it is not enough to claim that it has achieved global recognition. The justification of this argument can be concluded that much room for further discussion because the issue is incomplete, although it seems that already has begun to be taken seriously in various world regions.

[1]Ibid.

As it explains Section III (A) (3), this is the approach, which has the Council of Europe in Convention on Cybercrime. The following section below considers this option, analyzing the principles that could be used to create such a sample or, in the phrase used in the usual way, a group of "consensual crimes".[1]

3. The Reasons and the Need for Criminal Law Regulating the Phenomenon of Cybercrime Terrorism in the Modern World

Undeterred by the possibility of arrest or prosecution, computer criminals around the world are omnipresent threat to the financial health of businesses, faith of their customers and growing threat to the security of countries and nations (Cyber Crime and Punishment? Archaic Laws Threaten Global Information, 2000). Nations are very concerned about cybercrime, and it is a concern common to many international organizations, including the United Nations, the G-8, European Union, NATO (Fidler, Pregent & Vandurme, 2016), and Council of Europe. Law enforcement officials cannot act against computer criminals, so long as many countries do not apply the laws, which criminalize activities in which country criminals are engaged in cybercrimes.

Admittedly, cyber terrorism or alternatively cyber security remains enormous challenge at national State level, for European community and international law regardless of the fact that stakeholders recognize the cyber threat. What is true is that cyber terrorism or cyber threat involves numerous principles of international law. Nevertheless, much of the international law principles are not clear or specifically addressing cyber terrorism and as such many principles of international laws were developed prior to the emerge of cyber terrorism and cyber security issues appeared on stage. As argued by Fidler, Pregent, & Vandurme (2016, p. 15) "the only category in which cyber-specific international legal rules exist is in the criminal realm, where, for example, the Council of Europe has produced the Convention on Cybercrime" as discussed above. Yet, this is not clear in most of the countries in the world viewing from internal point of view. The indication is that none of the exiting current legal structure on cyber terrorism would be able to addresses effectively such acts.

The difficulty lies in how to define the laws that are needed to enable the capture and prosecution of computer criminals. Although it seems a simple task, here are

[1]Ibid.

raised difficult issues. One of the issues is whether the scope of the definition of computer crime laws should include only that prohibit activities that target computers or need to outlaw crimes against individuals have also been influenced by computers, such as computer tracking and terrorism computer. Another issue is whether these laws must be specific to only cybercrime targeting and crimes committed using computer technology.

Effective law enforcement is complicated by the transnational nature of the computer space and cooperative mechanisms beyond national borders to solve and prosecute crimes are complex and slow. Computer criminals can defy the conventional areas of jurisdiction of sovereign nations, creating attack almost every computer in the world, passing it across multiple national boundaries, or by designing attacks that seem to stem from foreign sources. Such techniques dramatically increase as the complexities of technical and legal ones investigation and prosecution of computer crimes[1].

Unlike traditional crime, cybercrime is a global crime. Crimes dealing with computers everywhere takes place in cybercrime space and do not stop at the conventional limits of states. They can be performed from any place and against any computer user in the world[2].

The national survey cited most frequently in the United States is "survey on cybercrime and security", which has been made by Computer Security Institute with the participation of the FBI's Team for Computer Intrusion branch in San Francisco.[3] The survey of CSI/FBI conducted annually since 1996, reports the results of the data provided by thousands of information security professionals employed in corporations, financial institutions, government agencies and

[1]The laws of most countries do not prevent computer crimes in a clear way. Territorial laws against physical acts of violation or breach of the peace and unauthorized access often did not include their "virtual"counterparts. Commercial websites as those hit recently by open denial of service and distributed shocks may not be included in the obsolete laws as a form of protected property. New types of crimes may belong to fracture as the Philippines learned when they tried to prosecute the author of Love Bug virus in May 2000.

[2]Communication from the Commission to the Council and the European Parliament, creates a safer information society by improving the security of information infrastructures and combating crime related to computers - 9 (2000), which is available at http://europa.eu.int/ISPO/ eif/InternetPoliciesSite/Crime/CrimeCommEN.html, hereinafter: the creation of a secure information society.

[3] For more information seeFinancial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar, Computer Security Institute (Mar. 12, 2001), http://www.gocsi.com/prelea_000321.htm.

universities (CSI/FBI, 2000). One area in which the survey investigates is the security breach if the interviewees respectively experienced information security breach in the last year. It noted that the number that is answered affirmatively has been increased yearly. In the 2001 survey, 85% of respondents said that over the past year have revealed violations, while only 42% of respondents to the 1996 survey reported having detected such violations. The survey shows, among other things, that (a) the Internet continues to be the growth point of attack,[1] (b) that the denial of service attacks is on the rise[2] and (c) viruses are constantly becoming common. Those who answered the survey of CSI/FBI are also required to assess the damage from the quantitative aspect of cybercrime attribute. The reported figures range from US $ 1.55 m in the 1997 survey to 3.77 million in the 2001 survey (Standler, 1999).[3]

Also, data from other countries reveal similar trends where "cybercrime is estimated half of all fraud committed in the United Kingdom (UK) in the first six months" of 2000, and had "increased by 56% of hacking in the United Kingdom during the past 12 months, with the majority of hackers seeking financial gain, for example by using hacking to hunt for money or for political reasons as it is with posting messages to a specific purpose in the company's website" (Ticehurst, 2000).

Statistics from China and Japan also showed dramatic increase in cybercrime, (Kabay, 2000)[4] and the version of the Australian survey of CSI/FBI found that "a

[1] In the 2001 survey, 70% reported that the Internet was a frequent point of attack, while only 59% reported this in the survey of 2000. See also financial losses due to interference of the Internet, theft of trade secrets and crimes of the other computer, ("For the fourth consecutive year, more people surveyed ... cited their Internet connection as a frequent point than their internal systems cited ....").

[2] Thirty-eight percent of those who responded to the survey in 2001 had revealed denial of service attacks, while only 27% of respondents to the 2000 survey reported the discovery of such attacks.

[3] Of course, some claim that it is difficult to estimate the amount of losses attributed to cybercrime.

[4] Official news agency Xinhua reported that cybercrime has marked an explosion in the People's Republic of China.

In Japan, the National Police Agency reported in February that cybercrime in 1998 was up 58% compared with 1997 - which marked a growth of 1300% since statistics were first kept in 1993. The specific crimes rose even even more than the average total amount, eg, data falsification and fraudulent cases in 1998 increased by 67%.

Chinese Public Security Department announced it had solved 100 criminal hacking cases in 1998, but this was only an estimation that about 15% of the current level of unauthorized access to the system. They said the reported computer crime was increasing at an annual rate of 30%. About 95% of all Chinese online systems were attacked last year, with many banks and other institutions targeted by criminal Chinese and international guests.

third of companies surveyed reported at least one attack during the past 12 months" (Deloitte, 1999)[1].

When interviewed people, they are asked about the future, "the number of those who said that virtual crime grow their concern is almost doubled," while those who said they are concerned about the displacement of crime against conventional property crimes dealing with computers has doubled. Apparently, it is difficult to gather accurate statistics regarding cybercrime. The problem in collecting data about the performance of computer crimes is that an unknown number of crimes of all kinds are undiscovered. Some frauds were discovered only after a long time since they took place and only a tenth of all crimes were committed with the use of computer systems[2].

When a country's laws punish crimes dealing with computers and they do not apply, then cooperation to solve a crime and the possibility of extradition a criminal in front of a court of the other country may not be possible. Inadequate regimes can protect criminals from law enforcement and criminals can go to a place without being punished, as they hinder the efforts of other countries to protect its citizens (U.S. Departament of Justice, 2000).

Conflicting national criminal laws were acceptable as long as the crime was limited and remained in low scale. A country's decision whether to incriminate the activities was a matter within the discretion of national, because the consequences of that decision will affect only those who live within the borders of that country. For example, before three hundred years, the chances of a French citizen, to find yourself in China was very small, whereas with the rapid spread of computer technology, which makes geographical borders are less important, people can cross borders in digital mode without passport and without having to use other aircraft or leave the bedroom. Indeed, by nature couplings and plaiting of routers and WWW-ve anyone can aim to visit a web-page site in France, but never realizing that his or her communication is traveled through Japan and Brazil to get there.

At a time when the world is slowly starting to deal with the traditional border crossings, the nature of space of the computer world is very contradictory with ground-based jurisprudence. Computer criminals can do games for children around

[1] The Australian survey found that attacks perpetuated were the case, "carried out without any preliminary plan", with no model of discrete detected in more than 75% of cases. According to respondents, motivation potential for an attack was curiosity (71%).

[2] Kruse, Heiser, op. cit. p. 10. dhe Accord Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, op. cit. p. 10.

the world, taking advantage of gaps in the criminal law and making mischief with fundamental impunity and citizens can be subject to prosecution in another country on the basis of its various laws (Inc, 2000).[1]

Conflict laws can lead to strange results for countries that have violated the rights of operators of amendment Internet web site. Presentation of cybercrime in his nature and interconnecting network makes it imperative for achieving sustainability in transnational criminal prohibitions. One of the ways to accomplish this is to create a single code of law that regulates the performance of computer crime anywhere in the world[2].

4. Adjustment of the Cybercrime Phenomenon of Terrorism in Some Countries European Union

In recent years, great strides have been made worldwide towards the development of information technology. Information and communication technology (Information and Communication Technology ICT) now permeates almost every aspect of people's lives in our country. The fact that society is based and is increasingly dependent on information technology and communication makes it exposed to terrorist threats through technology and threats to computer crimes, namely crimes against computer data and systems or through them.

European Union countries have achieved some progress in terms of criminal law regulating the phenomenon of computer terrorism. Also, some of these countries have adopted their own laws to penalize the perpetrators of cybercrime. These countries have developed a proper legal framework to detect, punish, deter and combat terrorism computer. We must emphasize that these countries are trying to find tools, methods and measures needed to prevent cybercrime, where efforts to regulate criminal and punish cybercrime actions. Below we present some data on criminal justice regulation, addressing the phenomenon of computer terrorism in some countries of the European Union.

[1]See also John F. McGuire, Note, When Speech Is Heard Around the World: Internet Content Regulation in the United States and Germany, 74 N.Y.U.L.REV. 750, 768-770,1999, available at http://www.nyu.edu/pages/lawreview/74/3/McGuire.pdf. (German prosecutors accused the executive of computer service as an accomplice to the spread of pornography and extremist propaganda based on the content of Internet news groups); Nancy Finken, Nebraska's Nazi, Nebraska Public Radio.

[2]Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime, Articles 4 – 15.

In Austria by law for the protection of private life, which entered into force on 1 January 2000, specified the penalties regarding illegal actions directed against the database. Under this law, shall be punished with fines for doing any of the following acts: (1) obtaining or maintaining voluntary access to illegal use of data; (2) intentional transmission of data in violation of Article confidentiality of data, especially if he or she has access for other purposes; (3) the use of data in violation of the legal decision or judgment by failing to correct false data or failing to deletion of data; and (4) the deliberate erasure of data[1].

In Belgium in November 2000, Parliament passed new legislation that included a range of new provisions in the Criminal Code that deal with Belgium cybercrime (Martin Donaghy)[2]. Their law, consider "computer forgery, computer fraud, hacking and sabotage as criminal offenses". Belgium law defined Computer Forgery in section 210 (b) of the Criminal Code and differs from that taken elsewhere: "Rather than discussing the quality of "a written document" in the data stored on a computer system," the new law criminalizes specific crime of counterfeiting software, which consists of "falsification of computerized information" (Criminal Code of Belgium, section 7 and 8). The new definition of the action does not "require specific purpose of material benefit or with intent to cause harm, fraud and sabotage". This includes the act of complete or attempt "to hide the truth through deliberate manipulation of computerized of the relevant legal data, or use of such data."

Unlike acts of counterfeiting, the new offense of computer fraud in Article 504 (4) requires that "computerized manipulation have procured pecuniary advantage rogue" to the perpetrator. Computer sabotage acts of incrimination in Article 550 (3), tells of the author acted to cause harm. It fulfills what has been a gap in the Criminal Code of Belgium.[3] While in the past, the notion of sabotage has sought the destruction or damage of physical objects. Destruction or damage to the computerized data does not regulate the existing penal code. Therefore, the new article criminalizes any manipulation of data with intent to cause damage[4].

[1] Martin Donaghy, Stanbrook & Hooper, International Centre for Commercial Law, http://www.icclaw.com/devs/belgium/it/beit_004.htm; Schjolberg, shënim i mësipërm 164.
[2] Martin Donaghy, Stanbrook & Hooper, International Centre for Commercial Law, http://www.icclaw.com/devs/belgium/it/beit_004.htm; Schjolberg, shënim i mësipërm 164.
[3] Ibid.
[4] Ibid.

Finland considers illegal creation and dissemination of computer viruses under the aegis of a criminal called "computer criminal damage"[1]. It has incriminated also computer fraud, and the damage that was done to computer data.[2] It also approved a list of provisions titled "data and communications minor" that consider illegal hacking and electronic communications interference.[3]

Germany has penalized computer sabotage[4], and computer fraud[5], together with data theft and modification or destruction of data[6]. While Greece's penal code protects the confidentiality and punishes anyone that copies, prints, uses or discloses illegally to a third party, or in any way violates the secret data or computer programs[7]; it also incriminates unauthorized access to computer systems and computer programs, and computer fraud.[8]

5. Adjusting the Criminal Law on Cyber Terrorism in Countries of Central Europe

The countries of Central and Eastern Europe have generally achieved less progress in terms of reforming their legal systems to incorporate computer crime, even though Russia is an exception. Russia has developed a broad legal framework to detect, punish and deter cybercrime, but its implementation remains problematic. Other countries of Central and Eastern Europe have, also begun to address cybercrime, as part of broader reforms in the region are ongoing. Romania and Poland have their bills in the process of processing that include provisions dealing with computers.

In the Federation of Bosnia and Herzegovina Criminal Code envisaged a provision for the punishment of theft of computer data (htt). Article 193 (2) of the Criminal Code, which entered into force on 20 November 1998, considers unlawful breach

[1] Finland Criminal Code, Chapter 34 § 9a, Enlist, available at http://www.urova.fi/home/oiffi/enlist/resources/penal.html.
[2] Ibid., chapter 35.
[3] Ibid., chapter 38.
[4]Germany Criminal Code § 303b, http://www.bmj.bund.de/publik/e_stgb.pdf.
[5] Ibid., chapter 263.
[6] Ibid., chapter 202 al.
[7] Issues Facing the Secure Links of CoCs: Derived Legal Issues, Cosacc Consortium, http://cosacc.acci.gr/d3_1/doc0015.htm (citing Greek Penal Code Article 370B).
[8] Ibid. (citing Greek Penal Code Article 370 C and Article 386 A). See Schjolberg, supra note 164, at Article 370C §2.

of the database computer containing personal data and stipulates the use of data and information from any other unauthorized person.[1]

Bulgaria's penal code also incriminated actions that include computers in separate categories, crimes against intellectual property and general economic crimes (Aippi.org). Article 172a, which regulates intellectual property crimes, criminalizes reproduction or distribution of someone else's property without the consent of the holder of the copyright.[2] The penalty for this type of crime is imprisonment up to 3 years and fines of 1000.00 to 3000.00 leva.[3] However, if the crime is a second offense, or if it causes substantial damage, the punishment is up to five years in prison and fines of 3000.00 to 5000.00 leva.[4]

In Slovenia, there is no specific legislation in force that deals with cybercrime (Code S. C., 2000). Slovenia expects soon to ratify the Convention on Cybercrime, which would oblige them to develop prosecution process for the offenses established by the convention. Slovenia's penal code allows the prosecution generally for all actions mentioned in the convention, although some minor amendments may be necessary to ensure full compliance with the convention. It is likely to make some amendments to the Criminal Procedure Code of Slovenia to comply with the convention (Code S. C., 2000).

In Albania, the use of computers and computer systems of public and private institutions has experienced rapid development and versatile. Currently some of the main public and private services are carried out through computer systems and Internet network and share of Internet access in Albania is growing more and more. Albania has ratified the Convention on Cybercrime, (Convention on cyber crime in Albania, 2002, p. 553) and for the implementation of the Convention, Albanian legislation has changed the Criminal Code of the Republic of Albania and has incriminated terrorist acts as well as new forms of criminality.

This code has changed in terms of increasing the articles that define cyber offenses in the field and on the basis of these changes, Computer Crime Division, responsible and concrete task, prosecution and investigation of offenses of this nature.

[1]Article 193 (2) reads as follows: (2) Whoever without authorization breaks into a computer data base containing personal data or makes them available to another, shall be punished by imprisonment for a term not exceeding six months.
[2] Ibid., neni 172 (a).
[3] Ibid.
[4] Ibid.

A study published in December 2000 found that Albania had no specific laws on cybercrime. The study noted also that the Albanian Authority for Regulation of Telecommunications had started talks "on the topic of cyber laws", aiming preparation of protocols of cooperation and exchange of information (MacConnell International, 2000).

6. Criminal Law Regulation of Computer Terrorism in Kosovo

In 1999, Kosovo has been under an international protectorate under Resolution 1244 and the issue of terrorism prevention in Kosovo was initially regulated by UNMIK Regulation 2001/12, in order to create specific legislation for the prosecution and punishment of perpetrators doing terrorist acts and other similar acts, including violent acts and acts dangerous to human life that are performed within and related to Kosovo.

After the declaration of independence of the Republic of Kosovo, the Assembly of the Republic of Kosovo in 2010 adopted the Law on preventing and combating cybercrime (Law Nr. 03/ L -166).This law aims to prevent and combat cybercrime with concrete measures, detection and sanction violations through computer systems, by providing observance of human rights and the protection of personal data.

This law applies to the entire territory of the Republic of Kosovo in the activities of computer systems, and is fully applicable to the storage of data in computer systems and establishes the methods and procedures on how and who can use these data. In addition, the Criminal Code of the Republic of Kosovo in Chapter XIV of Criminal offenses against the constitutional order and security of the Republic of Kosovo includes terrorism offenses (Code K. C., 2012).

Besides a large number of offenses against the information and communication technology or through it, a growing number of other major issues that end up in court involve electronic evidence that is stored on a computer system or other device. Thus, the justice system, especially judges and prosecutors must be prepared to cope with cyber terrorism cases and computer crimes involving electronic evidences.

The specific character of cybercrime, his great risk of social and permanent increase in their abuse requires that certain legal provisions regulate this issue. This should be understood, first of all, the need incriminations in new criminal code,

which would sanction criminal activity adequately. However, the speed at which the reform becomes law in this regard is inadequate, comparing the time at which appear cybercrime offenses. It is almost imposibe that side by side with development and the appearance of crybercirm offences to achieve to regulate on time the cirminal law legislation as a prevention rom these harmful social phenomenon(Vesel, 2009, p. 342). Finally, it should be noted that many countries are trying to find tools, methods and measures how best to prevent cybercrime. In the first place, efforts to regulate the criminal law, in particular the criminalization of certain acts cyber terrorism as criminal acts (Ragip, 2008, p. 215). Ministry of Internal Affairs of Kosovo has signed cooperation agreements with various countries for the purpose of police cooperation in all areas of combating crime and the Kosovo Police is implementing these agreements efficiently. In the fight against terrorism, the Republic of Kosovo has in effect a wide legislative base including (www.kosovo-assamby.com/laws), Figure 1:

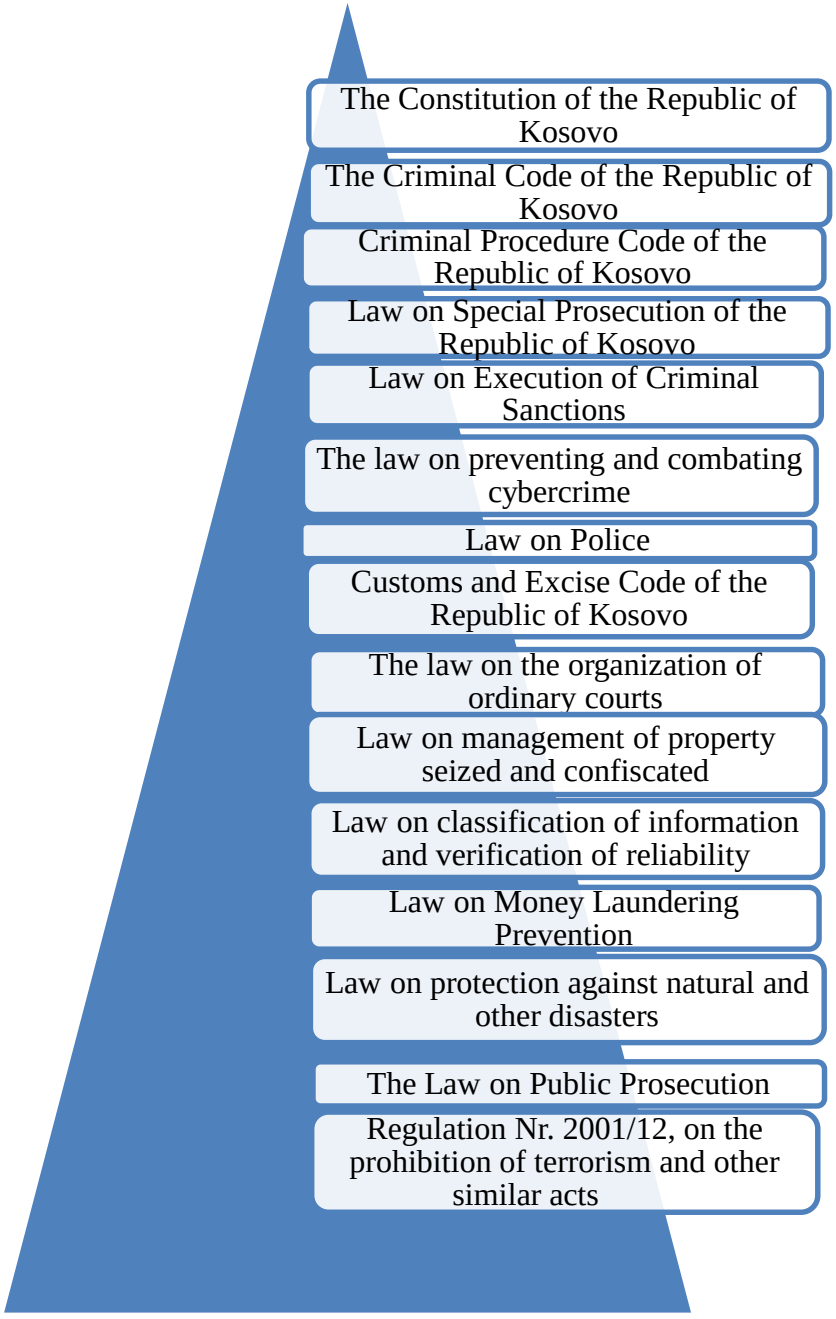

Figure 1. The legislative base of Kosovo

Also, there are international conventions and acts applicable in the Republic of Kosovo, related to the fight against terrorism, such as:

• Universal Declaration of Human Rights;

• European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols;

• Convention against Torture and Other Cruel, inhuman and degrading.

The Government of Kosovo has undertaken a number of initiatives to enhance its cooperation within the region, connected with computer terrorism. Also, in June 2010, the Parliament adopted the Law on preventing and combating cybercrime and the prevention, detection and sanction violations through computer systems, by providing observance of human rights and the protection of personal data. This law is fully applicable to the storage of data in computer systems and establishes the methods and procedures on how and by whom these data may be used. Under this law, the person's actions are considered unauthorized actions, if the person is not authorized by law or contract, if it exceeds the limits of the authorization and no permission from a competent and qualified, by law, to use, administer or control computer system, or to carry out scientific research in a computer system.(Law on prvention and combating cyber crime in Kosovo (Law no. 03/L-166) article 22 (1)).

In order to ensure a permanent international cooperation in the field of cybercrime, the Government of Kosovo has made available and a permanent contact office, which functions within the government. The purpose of this office contact in the Government of Kosovo is to provide specialized assistance and information on the legislation in the field of cybercrime as well as informs contact offices of other countries. This office assists in execution by legal provisions, in cases of combating cybercrime, cooperating with all competent authorities in Kosovo.(Law on prvention and combating cyber crime in Kosovo (Law no. 03/L-166) article 22 (1)).

On this legal basis that the Republic of Kosovo has and the establishment of institutions that have arisen from these laws, Kosovo has made some modest progress in preventing and combating terrorism in general and cyber terrorism in particular.

Computer terrorism as socially dangerous phenomenon is a reality for the world community and our state. Electronic management of technological processes in our

country, the transition to a large extent will result in new types of crimes, including terrorism Electronics. So, an effective international legal regime should also explicitly recognize the importance of international cooperation. In this regard, it should focus not only on building proper relationships with the other law enforcement and regulatory agencies, but also with the advice of other countries and, where appropriate for the review of national criminal and international cooperation and assistance more quickly and effectively connected with computer terrorism.

Terrorism at large and other related crimes have to find clear expression in domestic legislation, precisely, in a non-discriminatory manner and without feedback.

Laws and regulations should be made available to the general public and must be applied consistently and with transparency by public authorities, including the police and judiciary. This would constitute a prerequisite for citizens to understand the law and, consequently, to adapt their behavior. It is equally important to ensure the basis for efficient and responsive actions against all forms of terrorism, including actions taken by the police, in accordance with the action of the rule of law and international standards of human rights.

All countries must agree to harmonize legislation regulating the terrorism provisions of international criminal law. Such an approach will serve as supplementary and explanatory laws, conventions, treaties or other documents existing and customary international law governing law for combating terrorism.

Therefore, such an approach would be in favor of the development and formalization of frameworks that deliberately specify what constitutes a terrorist attack since there is no unified definition. Moreover, harmonization of legislation is in the mutual interest of countries to develop a predictable legal framework against terrorism. Intersectional cooperation is also needed among legal experts, political, military, technicians and experts in other fields of expertise to combine methods and solutions of each field in a "computer shield" effective.

National provisions for cooperation should support international legal framework for harmonization with Internet service providers, to data exchange and partnerships. From the perspective of international cooperation, the fact that an operation when it comes to terrorism computer is performed via computer infrastructure located in a state creates an obligation to cooperate with the state of the victim and this will be the choice of harmonization of legislation. In this regard,

it should focus not only on building proper relationships with other countries for law enforcement, but also to encourage other countries where it is appropriate to review the criminal and civil codes and their national remedial measures to make it more effective international cooperation and assistance.

7. Concluding Remarks

I conclude that indeed cyber terrorism is not regulated in line with international criminal law. Thus, I distinguish my conclusion and the risk it entails cyber terrorism due to lack of clear regulation addressing the issue, by citing the words of Dorothy Denning talking to the Special Oversight Panel on Terrorism of the Committee on Armed Services of the U.S. House of Representatives who concluded: "[f]or a terrorist, it would have some advantages over physical methods. It could be conducted remotely and anonymously, and it would not require the handling of explosives or a suicide mission. It would likely garner extensive media coverage, as journalists and the public alike are fascinated by practically any kind of computer attack. Indeed cyber terrorism could be immensely appealing precisely because of the tremendous attention given to it by the government and media" (Denning, 2000).

Against this background, due to lack of well-defined regulation of international criminal law to address cyber terrorism globally, there is no doubt cyber terrorism phenomenon will become more complex to be addressed by a set of international criminal law. Establishing legal basis globally against cyber terrorists and cyber criminals are essential. As noted above, states addresses cyber terrorism to some extent within their reach from different angles, nevertheless, as the cyber terrorism phenomenon is not an issue that may be dealt by a particular country alone, so it becomes necessary the cyber terrorism phenomenon to be regulated from a boarder perspective in line with international criminal law. Necessity to regulate cyber terrorism is determined from the perception of victim-States and their inability to punish cyber criminals.

Despite difficulties associated with the cyber menace line, it rests part of cyber security policy and law both at national and international levels, even where the law applied entails only of hangover regulations. It remains to be seen how and to what extent countries will be willingly to regulate cyber terrorism globally in line with international criminal law.

8. References

Alexander, Y. (2002). *Combating terrorism: strategies of ten countries*. University of Michigan Press.

Computer Security Institute (2001, March). *Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar*. Retreived from http://www.prnewswire.com/news-releases/financial-losses-due-to-internet-intrusions-trade-secret-theft-and-other-cyber-crimes-soar-71628527.html.

***Convention on Cyber Crime, ratified with law nr. 8888, dated 25/04/2002, official nr. 18, dated 17/05/2002, p. 553.

Council, O.E. (2001). *Convention on Cybercrime*. Budapest, November, 23.

Crime, C. (2000).and Punishment? Archaic Laws threaten global information. *McConnell International*.

***Criminal Code of Albania http://pbosnia.kentlaw.edu/resources/legal/albania/crim_code.htm.

***Criminal Code of Belgium.

***Criminal Code of Finlad. Retreved from *http://www.urova.fi/home/oiffi/enlist/resources/penal.html*.

***Criminal Code of Germany. Retreved from *http://www.bmj.bund.de/publik/e_stgb.pdf*http://www.ohr.int/ohr-dept/legal/crim-codes/default.asp?content_id=5130.

*** Criminal Code of Kosovo (2012, April) Code Nr. 04/L-82.

*** Criminal Code of Slovenia, (2000). Retreved from http://www.oecd.org/pdf/M00024000/M00024167.pdf.

***CSI/FBI (2000).Computer Crime and Security Survey, retreved from *http://www.cbc.ca/news/indepth/hackers/csifbi2000.pdf*.

***(1999). Deloitte and Victoria Police Computer Crime Survey. Retreved from Diaz-Paniagua, C. F. (2008). Un counter-terrorism treaties, 1997-2005. *Doctoral dissertation*, The City University of New York.

***(2001). *Economic and Social Council*. Conclusions of the Study on Effective Measures To Prevent and Control High-Technology and Computer-Related Crime.

Ermet, M. (2010, March). *Competition for Cybercrime Convetion of the Council of Europe. Heise Secirity*. Retreived from https://owl.english.purdue.edu/owl/resource/560/10/.

***FBI: *Raport financiar i krimeve për publikun*, 2010.

Fidler, D.P.; Pregent, R. & Vandurme, A. (2016). NATO, Cyber Defense, and International Law. *Journal of International and Comparative Law*, 4(1), 1.

Halili, R. (2011). *Kriminologjia/Criminology*. Prishtinë.

Ticehurst, Jo (2000, June). *Cybercrime Soars in the UK*. Retreved from *http://www.vnunet.com/News/1113497*.

Kabay, M.E. (2000, December). *Studies and Surveys of Computer Crime*. Security Portal.

Latifi, V. (2009). *Kriminalistika/Criminology*. Prishtinë.

Law Nr. 03/ L -166, Assambly of Kosovo.

Law Nr. 03/L-166. The law on preventing and combating cyber crimes in Kosovo . www.assembly-kosova.org

League Against Racism and Anti-Semitism v. Yahoo! Inc., No. RG: 00/05308 (County Ct. of Paris, Nov. 2000), retreived from *http://www.kentlaw.edu/perritt/conflicts/yahooparis.html*.

Martin, Donaghy & Stanbrook, Hooper, *International Centre for Commercial Law*, *http://www.icclaw.com/devs/belgium/it/beit_004.htm*; Schjolberg, shënim i mësipërm 164.

McGuire, J.F. (1999). When Speech Is Heard around the World: Internet Content Regluation in the United States and Germany. *NYUL Rev*., 74, p. 750.

(2000). President's Working Group on Unlawful Conduct on the Internet. *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the use of dhe Internet 41*.

Saul, B. (2008). Defining Terrorism to Protect Human Rights. *Sydney Law School Legal Studies Research Paper* No: 08-125.

Standler, R.B. (2002). *Computer crime.* Retrieved from http://www.rbs2.com/ccrime.htm.

Twellfth United Nation Congress on Crime Prevention and Criminal Justice. Comprehensive strategies for global challenges: crime prevention and criminal justice systems and their development in a changing world, A/CONF. 213/9 Salvador, Brazil, 12-19 april 2010. Retreived from http://www.un.org/en/conf/crimecongress2010/.

(2001). U.S. Department of Justice.

United Nations (2010). *Latin American and Caribbean Regional Meeting Report*.

Sources Online

http://www.aippi.org/reports/q169/q169_bulgaria_e.html.

http://www.deloitte.com.au/internet/item.asp?id=3140.

http://www.securityportal.com/cover/coverstory20001211.html.

http://www.usdoj.gov/criminal/cybercrime/unlawful.pdf.