The Budapest's Convention as a guarantee limit against cybercrime

By Eleni D. Chrysopoulou
J.D., Department of Law, Democritus University of Thrace, Greece,
B.Sc., M.Sc., Department of Applied Informatics, University of Macedonia, Greece.

1. Introduction

The vertiginous growth of the Internet has dramatically changed the way entities interact. Cyberspace enables people to share ideas over great distances and engage in the creation of an entirely new, diverse and chaotic democracy, free from geographic and physical constraints [Aldesco I.A., 2002]. The rapid progress of information technology has achieved significant advances in processing and transmitting data through use of computers and computer networks resulting in substantial benefits to society, including the ability to communicate with others real-time, access a library of information and transmit data instantly [Hopkins L.S., 2003].

The dark side of the above phenomenon is the fostering of new kinds of crimes, additional means to commit existing crimes and increased complexities of prosecuting crimes, since historical obstacles to international crime, such as distance, time and space, have now been eliminated. This international element in the commission of crime, whether it be traditional or new technological computer crime, creates new problems for both legal policy and law enforcement.

The above described challenge resulted in the Budapest's Convention, which with respect to human rights, aims at the adoption of appropriate and adequate international legal measures by the contracting countries.

The Convention on cybercrime provides a treaty-based framework that imposes on the participating nations the obligation to enact legislation criminalizing certain conduct related to computer systems, create investigative procedures and ensure their availability to domestic law enforcement authorities to investigate cybercrime offenses, including procedures to obtain electronic evidence in all of its forms and create a regime of broad international cooperation, including assistance in extradition of fugitives sought for crimes identified under the Convention [Marshall J.J., 2005].

2. The Cybercrime Convention

2.1 Importance of the Convention

A treaty, according to Article 2 of Vienna Convention, is "an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation" [Council of Europe]. Treaties are the only machinery that exist for adapting international law to new conditions and strengthening the force of a rule of law between states [Brierly J.L., 1963]. Thus, and taking into account the Council's of Europe declaration of the need to pursue a common criminal policy aimed at the protection of the society against cybercrime [Preamble, par.4], it seemed very important for an international regime to be set up to combat these types of crimes in a growing and integrated global society.

2.2 The way to the Convention

Before the Budapest's Convention adoption, a number of Committee of Ministers Recommendations' had been issued in an attempt to combat cybercrime. These Recommendations, also mentioned in the Convention's Preamble, are Committee of Ministers Recommendations No. R (85) 10, concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2, on piracy in the field of copyright and neighbouring rights, No. R (87) 15, regulating the use of personal data in the police sector, No. R (95) 4, on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9, on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13, concerning problems of criminal procedural law connected with information technology.

The Council of Europe's Convention on Cybercrime and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109th Session on November 8, 2001 and the Convention was opened for signature on November 23, 2001.

Negotiations on the Convention began in 1997, following a determination by the Council that the transnational character of cybercrime could only be tackled at the global level. To date, the Convention has been signed by 43 Council of Europe members and four non-members (Canada, Japan, South Africa and the United States) that also participated in the negotiations [Appendix]. It has also been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

Greece signed the Convention on 23.11.2001, but has yet to ratify it. Although, some provisions of the Convention are already covered by existing Greek domestic legislation, there still is a long way ahead. The distance will be covered with the Convention's critical and careful incorporation into the Greek legal order.

2.3 Objectives of the Convention

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

As recognized in the Convention's Preamble, the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks and the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks, require co-operation between States and private industry in combating cybercrime and increased, rapid and well-functioning international co-operation in criminal matters.

Moreover, the Council of Europe is mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties and also mindful of the right to the protection of personal data.

The Convention, as it is declared in its explanatory report, aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation [Explanatory Report, par.16].
Thus, the Convention's main goal is to establish a "common criminal policy" to better combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation. To these ends, the Convention is broken up into four main chapters: The first chapter defining the terms to be used, the second chapter referring to the measures to be taken at the national level, containing substantive law, procedural law and jurisdiction measures, the third chapter referring to the international cooperation and the fourth chapter, regarding the final provisions of the Convention.

2.4 The definitions of the Convention

Article 1 initially defines four terms vital to the treaty. The first term defined is "computer system", which is a device consisting of hardware and software developed for automatic processing of digital data [Explanatory Report, par.23]. For the purposes of this Convention, the definition of "computer data" builds upon the ISO-definition of data and must be in a form suitable for processing in a computer system [Explanatory Report, par.25]. The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems. This definition includes both public or private entities and "those entities that store or otherwise process data on behalf of public or private entities" [Explanatory Report, par. 26, 27]. The fourth defined term is "traffic data" which means data that is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself. When a Convention Party investigates a criminal offence within this treaty, traffic data is used to trace the source of the communication. Traffic data lasts for only a short period of time and the Convention makes Internet Service Providers (ISPs) responsible for preservation of this data [Explanatory Report, par. 28-31].
It is noted that Convention Parties would not be obliged to copy *verbatim* into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation [Explanatory Report, par.22].

3. Substantive law issues

Although there is an internationally continuing discussion "on just what constitutes a computer crime", there is yet no generally accepted definition of the term. The Convention on cybercrime supports this effort to define computer crime by including an array of different computer related offences in its substantive criminal law provisions [Viano C.E., 2004].

3.1 Confidentiality, integrity and availability offences

The purpose of this section of the Convention (Section 1, Articles 2-13) is to establish a common minimum standard of relevant offences so as to improve the means to prevent and suppress computer- or computer-related crime. Correspondence in

domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too [Explanatory Report, par.33].
As stated in the Explanatory Report, All the offences contained in the Convention must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. The drafters of the Convention agreed that the exact meaning of 'intentionally' should be left to national interpretation [Explanatory Report, par.39].
The criminal offences in Articles 2-6 were intended by the drafters to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices [Explanatory Report, par.43].

Illegal access
"Illegal access" covers the basic offence of dangerous threats to and attacks against the security, meaning the confidentiality, integrity and availability of computer systems and data. Examples of unauthorised acts of intrusion, which should be in principle illegal are "hacking", "cracking" or "computer trespass". Such intrusions may give access to confidential data, like passwords, information about the targeted system and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.
The act must also be committed "without right", meaning that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it, such as for the purpose of authorised testing or protection of the computer system concerned [Explanatory Report, par. 44, 47].

Illegal interception
This provision aims to protect the right of privacy of data communication. The offence which is criminalized is the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The provision is based upon the right to privacy of correspondence of the Article 8 of the European Convention on Human Rights and the offence of "unauthorised interception" described in Recommendation (89) 9. The offence established at this point applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer and applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission process and not the nature of the data transmitted, meaning that the data communicated may be publicly available information, but the parties wish to communicate confidentially or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right" [Explanatory Report, par. 51, 52, 54, 58].

Data interference
The acts of damaging, deletion, deterioration, alteration or suppression of computer data is, under this provision, punishable, if committed without right in a way that computer data and computer programs are protected the same way to that enjoyed by corporeal objects against intentional infliction or damage. The offender, here, must have acted "intentionally", too [Explanatory Report, par. 60, 63].

System Interference
The criminalization of the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data is based upon the "computer sabotage" of the Recommendation No. (89)9. The "hindering" must be "without right" and "serious" and the offence must be committed "intentionally" in order to give rise to criminal sanction [Explanatory Report, par. 65, 67, 68, 70].

Misuse of devices
This article establishes, as separate and independent offences, the intentional commission of illegal acts regarding certain devices that are used in the commission of the named offences of this Convention. The article intends to combat black markets which are established to facilitate the sale or trade of "hacker tools," or tools used by hackers in the commission of cybercrimes by prohibiting the production, sale, or distribution of these devices. The drafters intended this Article to relate to devices that "are objectively designed, or adapted, primarily for the purpose of committing an offence". Finally, in order to avoid overcriminalization, Article 6 requires both a general intent and also a "specific… intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention" [Explanatory Report, par. 71, 72, 73, 76].

3.2 Computer-related offences
The purpose of Article 7, which outlaws computer-related forgery, is to create a parallel offence to the forgery of tangible documents. It is also noted that national concepts of forgery vary greatly, but, it was agreed that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term "authentic" the genuineness of the data, if they choose so [Explanatory Report, par. 81, 82].
Article 8 makes computer-related fraud illegal. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property and its objective is to protect assets represented or administered in computer systems, such as electronic funds and money deposits. The computer fraud manipulations are criminalised if they are committed "intentionally", "without right" and moreover, produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person [Explanatory Report, par. 86, 89, 90].

3.3 Content-related offences
Article 9 tries to strengthen and modernize the existing criminal law provisions against sexual exploitation of children and expand them to electronic transmissions. The described illicit acts related to child pornography must be criminalized by the Parties if committed "intentionally".
This provision responds to the preoccupation of Heads of State and Government of the Council of Europe, expressed at their 2nd summit (Strasbourg, 10 – 11 October 1997) in their Action Plan (item III.4) and corresponds to an international trend that seeks to ban child pornography, as evidenced by the recent adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child

prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography (COM2000/854).
It criminalises various aspects of the electronic production, possession and distribution of child pornography to combat the new form of sexual exploitation and endangerment of children via the internet. Paragraph 1(a) criminalises the production of child pornography for the purpose of distribution through a computer system, when paragraph 1(b) criminalises the "offering" of child pornography through a computer system and also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography. Paragraph 1(c) criminalises the distribution or transmission of child pornography through a computer system, when in paragraph 1(d), actively obtaining child pornography, for example by downloading it, is criminalised. The possession of child pornography in a computer system or on a data carrier is criminalised in paragraph 1(e). [Explanatory Report, par. 91, 92, 94-98, 105]
The three types of pornographic material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although "realistic", do not in fact involve a real child engaged in sexually explicit conduct (2c).
Paragraph 3 defines the term "minor" in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a 'child' in the UN Convention on the Rights of the Child (Article 1). Nevertheless, the provision allows Parties to require a different age-limit, provided it is not less than 16 years [Explanatory Report, par. 94-102,104].

3.4 Infringements of copyright and related rights

Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet. Such protected works include literary, photographic, musical, audio-visual and other works. Each Party is obliged to criminalise wilful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale. Copyright and related rights offences must be committed "wilfully" for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term "wilfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement (Article 61), governing the obligation to criminalise copyright violations [Explanatory Report, par. 107, 108, 113].

3.5 Attempt and aiding or abetting

This article relates to offences dealing with intentionally attempting or aiding and abetting "the commission of the offences defined in the Convention". Liability under Article 11 arises when "the person who commits a crime established in the Convention is aided by another who also intends that the crime be committed". With respect to paragraph 2 on attempt, some offences defined in the Convention, or elements of these offences, were considered to be conceptually difficult to attempt, like for example, the elements of offering or making available of child pornography. According to the provision, it is only required that the attempt be criminalised with

respect to offences established in accordance with Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c) [Explanatory Report, par. 118-122].

3.6 Corporate Liability

Article 12 deals with the liability of legal persons. Here, liability is imposed on corporations, associations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 also contemplates liability where such a leading person fails to supervise or control an employee or an agent of the legal person, where such failure facilitates the commission by that employee or agent of one of the offences established in the Convention. Under paragraph 1, four conditions need to be met for liability to attach, when under paragraph 2 Parties are obliged to have the ability to impose liability upon a legal person where the crime is committed not by the leading person described in paragraph 1, but by another person acting under the legal person's authority. Liability under this Article may be criminal, civil or administrative. Paragraph 4 clarifies that corporate liability does not exclude individual liability [Explanatory Report, par. 123-127].

3.7 Sanctions and measures

This provision requires that the Convention Parties provide criminal sanctions that are "effective, proportionate and dissuasive" and "include the possibility of imposing prison sentences" [Explanatory Report, par. 128].

4. Procedural law issues

The Convention defines powers to facilitate criminal investigations.

4.1 Scope of procedural provisions

The articles in this section describe procedural measures that Convention parties must take "at the national level for the purpose of criminal investigation of the offences established in Section 1".

Electronic data may very well be the only evidence in a criminal investigation. One way in which the Convention overcomes the problem of the speed and the easiness that this evidence can be altered, moved, or deleted, is by adapting traditional procedures, like search and seizure, to an ever-changing technological landscape. However, in order to make these traditional crime investigation methods effective, new measures have been created, such as the expedited preservation of data, the real-time collection of traffic data, and the interception of content data [Explanatory Report, par. 131, 134].

4.2 Conditions and safeguards

The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. The minimum safeguards to which Parties to the Convention must adhere include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005, 009, 046, 114, 117 and 177), in respect of European States that are Parties to them and also, other applicable human rights instruments in respect of States in other regions of the world which are Parties to these instruments, as well as the more

universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.
Another safeguard according to this article is that the powers and procedures shall "incorporate the principle of proportionality" [Explanatory Report, par. 145, 146].
Opponents to the Convention argue that the treaty infringes upon basic human rights and liberties, with the most significant of them to be, the right to privacy.

4.3 Expedited preservation of stored computer data
Article 16 introduces a new measure in order to facilitate the investigation of cybercrimes. This measure, so as the other one referred in Article 17, apply to stored data, that has already been collected and stored at data holders and not to real time data. [Explanatory Report, par. 149].
Here, it has to be mentioned that while "data preservation" means keeping data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate, "data retention" means keeping data, which is currently being generated, in one's possession into the future. On the one hand, data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe. Articles 16 and 17 refer only to data preservation, and not data retention [Explanatory Report, par. 151, 152].
Data preservation is for most countries an entirely new legal power or procedure in domestic law, as it is an important new investigative tool in addressing computer and computer-related crime, especially crimes committed through the Internet. The statute operates in either by the way in which the competent authorities in the Convention party country simply access, seize and secure the relevant data, or by the way in which, where a reputable business is involved, competent authorities can issue an order to preserve the relevant data. Convention parties are thus required to introduce a power that would enable law enforcement authorities to order the preservation of data for a particular period of time not exceeding 90 days. It is also noted that preservation measures exist at the national level in order to enable Parties to assist one another at the international level with expedited preservation of stored data located in their territory [Explanatory Report, par. 155-157].

4.4 Expedited preservation and partial disclosure of traffic data
This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service. Obtaining stored traffic data that is associated with past communications may be critical in a criminal investigation. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service providers. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted [Explanatory Report, par. 165-169].

4.5 Production order
This provision relates to production orders, which specifically allow "competent authorities to compel a person in its territory to provide specified stored computer

data" or to compel an Internet Service Provider to provide subscriber information. Article 18 relates exclusively to production of stored or existing data. Production orders precede search and seizure as a means of obtaining specific data. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorise Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers, like for example, for the purpose of data-mining. [Explanatory Report, par. 170, 175, 182].

4.6 Search and seizure of stored computer data

This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Domestic legislations include powers for search and seizure of tangible objects. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data, even if it *per se* will not be considered as a tangible object.

With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain, with the preconditions for obtaining legal authority to undertake a search remaining the same. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. In the case of electronic data either the physical medium on which the intangible data is stored must be seized or taken away, or a copy of the data must be made in either tangible form, such as a computer printout, or in intangible form, such as a diskette, before the tangible or intangible medium containing the copy can be seized and taken away [Explanatory Report, par. 184, 186, 187].

4.7 Real-time collection of traffic data

Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings. Like real-time interception of content data, real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Thus, Internet Service Providers and their employees knowing about the interception must be under an obligation of secrecy in order for the procedure to be undertaken effectively. Paragraph 3 obligates Parties to adopt such legislative or other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data. Paragraph 3 may be affected by the creation of explicit obligations in the law [Explanatory Report, par. 216, 225, 226].

4.8 Interception of content data

Traditionally, the collection of content data in respect of telecommunications, for example, telephone conversations, has been a useful investigative tool to determine that the communication is of an illegal nature.

Given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound and that the communication through the Internet tends to be the most popular way of communication, it has greater potential for committing crimes involving distribution of illegal content. “Content data” refers to the communication content of the communication, which is the meaning of the communication, or the message or information being conveyed by the communication [Explanatory Report, par. 228, 229].

5. Jurisdiction and international cooperation

Article 21 establishes that Parties must enact laws so that they have jurisdiction of all the crimes described in the Convention if they occur in any of the four places the article mentions. In case more than one Party has jurisdiction over some or all of the participants in the crime, the affected Parties are to consult in order to determine the proper venue for prosecution where appropriate [Explanatory Report, par. 239]. Countries, however, are not bound to accept these possible ways to attain jurisdiction and, thus, countries like the United States, that seldom premises jurisdiction upon a nationality principle could easily ignore nationality as a base for acquiring jurisdiction [Viano C.E., 2004].

Chapter III (Articles 23- 35) contains a number of provisions relating to extradition and mutual legal assistance among the Parties. This was a significant point of the Treaty cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries. As Professor James Boyle noted, “If the king’s writ reaches only as far as the king's sword, then much of the content on the Internet might be presumed to be free from the regulation of any particular sovereign", an observation which is particularly apt in the criminal enforcement context [Weber M.A., 2003].

Considering that it is impossible to regulate criminal behaviour without a means to ensure enforcement of sanctions, the objective of the drafters at this Chapter was to extend the ambit of the king's sword through cooperation.

Article 23 sets forth three general principles with respect to international co-operation. First, it declares that international co-operation is to be provided among Parties "to the widest extent possible". Second, it mentions that co-operation is to be extended to all criminal offences related to computer systems and data, as well as to the collection of evidence in electronic form of a criminal offence, meaning that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system involves electronic evidence, the terms of Chapter III are applicable.

However, it should be noted that Article 24 (Extradition), according to which the obligation to extradite applies only to those crimes committed in Articles 2- 11, Article 33 (Mutual assistance regarding the real time collection of traffic data), according to which each Party is obliged to collect real time “traffic data” for another member country and Article 34 (Mutual assistance regarding the interception of content data), which discusses the cooperation and sharing of information obtained through means as eavesdropping and wiretapping, permit the Parties to provide for a different scope of application of these measures.

Third, it states that co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws".

Article 25 requires mutual assistance “to the widest extend possible”, when Article 26, referring to those cases when a Party obtains important information that may assist

another member country in a criminal investigation, calls them "spontaneous information". Article 27 discusses mutual assistance in the case of absence of applicable international agreements. Article 28, which is applicable only when no mutual assistance treaty exists, provides for confidentiality and limitations on use of information, so as to preserve sensitive materials of a host country. Article 29 is the same as Article 16, except that it refers to international cooperation. Likewise, Article 30, is the mutual assistance version of Article 17. Article 31 requires that each member country have the ability to search, access, or seize "data stored by means of a computer system located within its territory" for the benefit of another member country. Article 32 merely makes it permissible for a source of data that already is publicly available to be available to a Party unilaterally and without a mutual assistance request, while at the same time, not preparing a comprehensive, legally binding system. Parties become, through Article 35, members of a 24/7 network, in order to face effectively crimes which require a rapid response.

Improving a state's legal ability to provide and receive international cooperation to face cybercrime effectively is not merely a question of improving its laws related to mutual assistance and extradition, but, there is a significant relationship between the legal ability to provide international cooperation and the quality of a state's laws that define crime, establish legal investigative powers and provide safeguards. In order for the states to achieve the above goal, a number o measures [Piragoff K.D., 2004] have been proposed.

6. Additional Protocol

The first Additional Protocol on Racism and Xenophobia on the internet (ETS 189) has been opened for signature in Strasbourg, January 26, 2003.

The Convention, as the most recent international instrument in its field, binds its ratifying Parties, shapes their domestic laws but also, functions as a model law for those Parties that consider to accede, or serve as a model law for other states. In particular, the substantive part is meant as a framework, where new and other IT-related misuse will be added to the Convention in the form of additional protocols, like this first one, so that the Convention gives its full effect, when these protocols come into force [Kaspersen W.K.H., 2004].

The Additional Protocol after defining "racist and xenophobic material" as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors", proposes, with its Articles 3-6 certain measures to be taken at national level so as to criminalize acts of a racist and xenophobic nature committed through computer systems. Article 7 criminalizes aiding and abetting the commission of any of the offences established in accordance with the Protocol, with intent that such offence be committed. Article 8, paragraph 1 states that Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol and paragraph 2 states that the Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol. Final provisions are included in articles 9-16.

7. Opposition to the Convention

The Convention on cybercrime, as any pioneering legal tool, faced severe criticism and opposition.

Among the arguments against the Convention is the claim that the Treaty restricts freedom of expression online.

Another argument against the Convention is that it overstrains the investigative powers of police forces and governmental organizations, meaning that that the government is granted an excessive amount of investigatory power, which is best illustrated in the example of call data vs. "traffic data".

Before the Treaty, law enforcement agencies were allowed to seek call related data, such as the phone numbers that are dialed and the duration of the calls. However, under the Convention, law enforcement authorities would have the right to wide-ranging "traffic data," which includes the source, destination, and duration of calls, as well as the type of traffic or the sort of services consulted. A point of discussion is whether it is a violation of privacy if an Internet Service Provider is forced to inform law enforcement agencies about the downloads, e-mails and duration of visits to particular websites a client did [Keyser M., 2003]. The American Civil Liberties Union claims that U.S. authorities will use the Convention to conduct surveillance and searches that would not be permitted under current U.S. law. European critics worry that the Convention allows the transfer of personal data to countries outside Europe–such as the United States–that they believe have less protective laws regarding the use of such information. Council of Europe officials dismiss such fears, arguing that the Convention provides adequate civil liberty safeguards and limits information transfers to specific criminal investigations [Archick K., 2002].

Another point of criticism is that the Treaty obliges companies and individuals to provide law enforcement with far greater information than is considered the norm under most telecommunications laws. ISPs and other related businesses keep "subscriber data", which is confidential client records and they are unwilling to offer them to an investigating governmental agency. Moreover, companies are concerned with the increased costs associated with retaining and preserving data should an order be served upon the company to do so and it is ultimately the consumer that will need to weigh the importance this cost [Keyser M., 2003]. Meanwhile, some business and consumer groups are concerned that the Convention's provisions that increase costs to service providers, impede the development of security technologies and sale of encryption programs, and negatively affect consumer confidence in e-commerce.

Another hot topic is that the Convention infringes upon citizen civil liberties. Article 15 requires member countries "to establish conditions and safeguards to be applied to the" governmental powers established in Articles 16 thru 21. Those conditions and safeguards are required "to protect human rights and liberties". Article 15 in fact "lists some specific safeguards, such as requiring judicial supervision, that should be applied where appropriate in light of the power or procedure concerned" [Keyser M., 2003].

The Global Internet Liberty Campaign (GILC), a non profit, non governmental organization, whose member organizations have joined together to protect and promote fundamental human rights such as freedom of speech and the right of privacy on the net for users all over the world, is strongly opposed to certain guidelines of the Treaty. GILC has drafted two letters against the Treaty's provisions because it believes that they run contrary to internationally accepted human rights norms and infringe on the free speech and privacy rights of all internet users [GILC, 2000].

On the other hand, some analysts criticize the Convention as being too "indulgent" or "soft", because of not permitting police authorities direct crossborder access to computer data, which they argue creates an extra, time-wasting step [Archick K., 2002].

Another point of consideration is that the states that participated in the Convention's negotiations are not the "problem countries" in which cyber criminals operate relatively freely. Hackers frequently route cyber attacks through portals in Yemen or North Korea, neither of which are part of the Convention, so sceptics point out that for the Convention, in order to serve as a deterrent, more states will have to sign it and abide by its mandates. As an example, it is noted that the Filipino author of the "I Love You" virus that caused millions of dollars in damage worldwide in 2000 was never prosecuted because no applicable laws existed **[**Archick K., 2002].

8. Conclusion

Computer crime, and especially cybercrime, is not a specific new form of crime, but rather a wide variety of new phenomena, which encompasses both new types of crimes, as well as traditional crimes committed in connection with computer systems or computer networks [Sieber U., 2004]. This represents a tremendous challenge for the criminal law.

The Convention on cybercrime is based on three pylons. First, it defines criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes–fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability. Second, it establishes domestic procedures for detecting, investigating, and prosecuting computer crimes, and collecting electronic evidence of any criminal offense. Such procedures include the expedited preservation of computer-stored data and electronic communications, search and seizure of system, and real-time interception of data. Third, it establishes a rapid and effective system for international cooperation. The Convention deems cybercrimes to be extraditable offenses, and permits law enforcement authorities in one country to collect computer-based evidence for those in another. It establishes a 24/7 contact network to provide immediate assistance with cross-border investigations.

Above all, parties to the Convention must guarantee the conditions and safeguards necessary to protect human rights and the principle of proportionality.

There is no doubt that the Treaty represents a flexible and effective vehicle in combating cybercrime and a useful tool in harmonizing the law and improving cooperation between legal systems in the field of computer crime. The fast changing nature of cybercrime, nevertheless, necessitates both the monitoring of future developments in computer crime and further analysis of new threats which the criminal law will be required to address [Sieber U., 2004]. Moreover, the sensitive nature of the fundamental human rights, such as the privacy and freedom of speech, require borders at the guidelines and the procedures which restrict them.

References

[Aldesco I.A., 2002] Aldesco I.A. (2002), The demise of anonymity: A constitutional challenge to the convention on cybercrime, Loyola of Los Angeles Entertainment Law Review, 81

[Hopkins L.S., 2003] Hopkins L.S. (2003), Cybercrime Convention: A positive beginning to a long road ahead, Journal of High Technology Law, 101

[Marshall J.J., 2005] Marshall J.J. (2005), The Convention on cybercrime: A harmonized implementation of international penal law: what prospects for procedural law process?, Comp. & Info. Law, 329

[Council of Europe] Council of Europe, Treaty Office, online at http://conventions.coe.int/Treaty/EN/v3Glossary.asp/accessed 11.10.2003

[Brierly J.L., 1963] Brierly J.L. (1963), The law of Nations: An introduction to the international law of piece 57, Humphrey Waldock ed., Oxford Univ. Press 6th ed.

[Preamble, par.4] Convention on Cybercrime, Preamble, online at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm/ accessed 03.04.2011

[Explanatory Report, par.##]. Convention on Cybercrime, Explanatory Report, online at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm/ accessed 03.04.2011

[Viano C.E., 2004] Viano C.E. (2004), Computer crimes and criminal law: international dilemmas and approaches, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 51-52, 67

[Weber M.A., 2003] Weber M.A. (2003), Berkeley Technology Law Journal, 425

[Piragoff K.D., 2004] Piragoff K.D. (2004), International cooperation in combating cyber-crime and cyber-terrorism, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 192-193

[Kaspersen W.K.H., 2004] Kaspersen W.K.H. (2004), Gathering electronic evidence, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 80-81

[Archick K., 2002] Archick K. (2002), CRS Report for Congress, Cybercrime: The Council of Europe Convention, online at http://www.usembassy.it/pdf/other/RS21208.pdf/accessed 10.04.2011

[Keyser M., 2003] Keyser M. (2003), Transnational Law and Policy Journal, Vol. 12. 12:2, 324-326

[GILC, 2000] GILC (2000), The letters drafted by GILC are available online at http://gilc.org/privacy/coe-letter-1000.html and http://gilc.org/privacy/coe-letter-1200.html/ accessed 15.03.2011

[Sieber U., 2004] Sieber U. (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 47-50

Appendix: Council of Europe Convention on Cybercrime

Chart of signatures and ratifications, ETS no 185.
Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other nom-member States.
Online at
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG/accessed 26.04.2011
Status as of 01.04.2011

Opening for signature
Place: Budapest
Date: 23.11.2001

Entry into force
Conditions: 5 Ratifications including at least 3 member States of the Council of Europe
Date: 01.07.2004

Member States of the Council of Europe

States	Signature	Ratification	Entry into force
Albania	23/11/2001	20/6/2002	1/7/2004
Andorra			
Armenia	23/11/2001	12/10/2006	1/2/2007
Austria	23/11/2001		
Azerbaijan	30/6/2008	15/3/2010	1/7/2010
Belgium	23/11/2001		
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006
Bulgaria	23/11/2001	7/4/2005	1/8/2005
Croatia	23/11/2001	17/10/2002	1/7/2004
Cyprus	23/11/2001	19/1/2005	1/5/2005
Czech Republic	9/2/2005		
Denmark	22/4/2003	21/6/2005	1/10/2005
Estonia	23/11/2001	12/5/2003	1/7/2004
Finland	23/11/2001	24/5/2007	1/9/2007
France	23/11/2001	10/1/2006	1/5/2006
Georgia	1/4/2008		
Germany	23/11/2001	9/3/2009	1/7/2009
Greece	23/11/2001		
Hungary	23/11/2001	4/12/2003	1/7/2004
Iceland	30/11/2001	29/1/2007	1/5/2007
Ireland	28/2/2002		
Italy	23/11/2001	5/6/2008	1/10/2008
Latvia	5/5/2004	14/2/2007	1/6/2007
Liechtenstein	17/11/2008		
Lithuania	23/6/2003	18/3/2004	1/7/2004
Malta	17/1/2002		
Moldova	23/11/2001	12/5/2009	1/9/2009
Monaco			
Montenegro	7/4/2005	3/3/2010	1/7/2010
Netherlands	23/11/2001	16/11/2006	1/3/2007
Norway	23/11/2001	30/6/2006	1/10/2006
Poland	23/11/2001		
Portugal	23/11/2001	24/3/2010	1/7/2010
Romania	23/11/2001	12/5/2004	1/9/2004
Russia			
San Marino			
Serbia	7/4/2005	14/4/2009	1/8/2009
Slovakia	4/2/2005	8/1/2008	1/5/2008
Slovenia	24/7/2002	8/9/2004	1/1/2005
Spain	23/11/2001	3/6/2010	1/10/2010
Sweden	23/11/2001		
Switzerland	23/11/2001		
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005
Turkey	10/11/2010		
Ukraine	23/11/2001	10/3/2006	1/7/2006
United Kingdom	23/11/2001		

Nom-member States of the Council of Europe

States	Signature	Ratification	Entry into force
Argentina			
Australia			
Canada	23/11/2001		
Chile			
Costa Rica			
Dominican Republic			
Japan	23/11/2001		
Mexico			
Philippines			
South Africa	23/11/2001		
United States of America	23/11/2001	29/9/2006	1/1/2007

Total number of signatures not followed by ratifications: 17
Total number of ratifications/ accessions: 30