Introduction and background:

Since early history human population and societies has been changing in characteristics, depending on their way of life like prominent jobs, tools, and communication. In the early ages it was gathering, hunting, agricultural, industrial, and now the age of Information Society “most of the people work with information related jobs, instead of dealing directly with physical objects”, for each kind of these societies it has also is related offences and crimes. 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. Cyber crime, especially, by adopting appropriate
legislation and fostering international co-operation.

The Convention is the product of four years of work by Council of Europe experts, but
also by the United States, Canada, Japan and other countries, which are not members of
the Organisation. An Additional Protocol making any publication of racist will
supplement it and xenophobic propaganda via computer networks a criminal offence.

Why we need Cyber Crime Convention

The revolution in information technologies has changed society fundamentally and will
probably continue to do so in the foreseeable future. Many tasks have become easier to
handle. Where originally only some specific sectors of society had rationalised their
working procedures with the help of information technology, now hardly any sector of
society has remained unaffected. Information technology has in one way or the other
pervaded almost every aspect of human activities. A conspicuous feature of information
technology is the impact it has had and will have on the evolution of telecommunications
technology. Classical telephony, involving the transmission of human voice, has been
overtaken by the exchange of vast amounts of data, comprising voice, text, music and
static and moving pictures. This exchange no longer occurs only between human beings,
but also between human beings and computers, and between computers themselves.
Packet-switched networks have replaced circuit-switched connections. It is no longer
relevant whether a direct connection can be established; it suffices that data is entered
into a network with a destination address or made available for anyone who wants to
access it. The pervasive use of electronic mail and the accessing through the Internet of
numerous web sites are examples of these developments. They have changed our society
profoundly. The ease of accessibility and search ability of information contained in
computer systems, combined with the practically unlimited possibilities for its exchange
and dissemination, regardless of geographical distances, has lead to an explosive growth
in the amount of information available and the knowledge that can be drawn there from.
These developments have given rise to unprecedented economic and social changes, but
they also have a dark side: the emergence of new types of crime as well as the
commission of traditional crimes by means of new technologies. Moreover, the
consequences of criminal behaviour can be more far-reaching than before because they
are not restricted by geographical limitations or national boundaries. The recent spread
of detrimental computer viruses all over the world has provided proof of this reality.
Technical measures to protect computer systems need to be implemented concomitantly
with legal measures to prevent and deter criminal behaviour

The new technologies challenge existing legal concepts. Information and
communications flow more easily around the world. Borders are no longer boundaries to
this flow. Criminals are increasingly located in places other than where their acts
produce their effects. However, domestic laws are generally confined to a specific
territory. Thus solutions to the problems posed must be addressed by international law,
necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society.

History and Preparatory work

By decision CDPC/103/211196, the European Committee on Crime Problems (CDPC) decided in November 1996 to set up a committee of experts to deal with cyber-crime. The CDPC based its decision on the following rationale:

- The fast developments in the field of information technology have a direct bearing on all sections of modern society. The integration of telecommunication and information systems, enabling the storage and transmission, regardless of distance, of all kinds of communication opens a whole range of new possibilities. These developments were boosted by the emergence of information super-highways and networks, including the Internet, through which virtually anybody will be able to have access to any electronic information service irrespective of where in the world he is located. By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.

- The criminal law must therefore keep abreast of these technological developments, which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse. Whilst Recommendation No. (89) 9 [3] resulted in the approximation of national concepts regarding certain forms of computer misuse, only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena. In the framework of such an instrument, in addition to measures of international co-operation, questions of substantive and procedural law, as well as matters that are closely connected with the use of information technology, should be addressed."

- In addition, the CDPC took into account the Report, prepared - at its request - by Professor H.W.K. Kaspersen, which concluded that "… it should be looked to another legal instrument with more engagement than a Recommendation, such as a Convention. Such a Convention should not only deal with criminal substantive law matters, but also with criminal
procedural questions as well as with international criminal law procedures and agreements." * A similar conclusion emerged already from the Report attached to Recommendation N° R (89) 9 ** concerning substantive law and from Recommendation N° R (95) 13 *** concerning problems of procedural law connected with information technology.

The new committee’s specific terms of reference were as follows:

"Examine, in the light of Recommendations No R (89) 9 on computer-related crime and No R (95) 13 concerning problems of criminal procedural law connected with information technology, in particular the following subjects:

- cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;

- other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;

- the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, e.g. via the Internet, search and seizure in information-processing systems (including Internet sites), rendering illegal material inaccessible and requiring service providers to comply with special obligations, taking into account the problems caused by particular measures of information security, e.g. encryption;

- the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (locus delicti) and which law should accordingly apply, including the problem in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;

- questions of international co-operation in the investigation of cyber-space offences, in close co-operation with the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC)."
Further to the CDPC’s decision, the Committee of Ministers set up the new committee, called "the Committee of Experts on Crime in Cyber-space (PC-CY)" by decision n° CM/Del/Dec(97)583, taken at the 583rd meeting of the Ministers’ Deputies (held on 4 February 1997). The Committee PC-CY started its work in April 1997 and undertook negotiations on a draft international convention on cyber-crime. Under its original terms of reference, the Committee was due to finish its work by 31 December 1999. Since by that time the Committee was not yet in a position to fully conclude its negotiations on certain issues in the draft Convention, its terms of reference were extended by decision n° CM/Del/Dec(99)679 of the Ministers’ Deputies until 31 December 2000. The European Ministers of Justice expressed their support twice concerning the negotiations: by Resolution No. 1, adopted at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the CDPC on cyber-crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as by Resolution N° 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cyber-crime. The member States of the European Union expressed their support to the work of the PC-CY through a Joint Position, adopted in May 1999.

Between April 1997 and December 2000, the Committee PC-CY held 10 meetings in plenary and 15 meetings of its open-ended Drafting Group. Following the expiry of its extended terms of reference, the experts held, under the aegis of the CDPC, three more meetings to finalise the draft Explanatory Memorandum and review the draft Convention in the light of the opinion of the Parliamentary Assembly. The Assembly was requested by the Committee of Ministers in October 2000 to give an opinion on the draft Convention, which it adopted at the 2nd part of its plenary session in April 2001. Following a decision taken by the Committee PC-CY, an early version of the draft Convention was declassified and released in April 2000, followed by subsequent drafts released after each plenary meeting, in order to enable the negotiating States to consult with all interested parties. This consultation process proved useful.

The revised and finalised draft Convention and its Explanatory Memorandum were submitted for approval to the CDPC at its 50th plenary session in June 2001, following which the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature.

Framework of the convention:

The Convention 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.

The Convention, accordingly, contains four chapters:

(I) Use of terms;

(II) Measures to be taken at domestic level - substantive law and procedural law;

(III) International co-operation;

(IV) Final clauses.

Section 1 of Chapter II (substantive law issues) covers both criminalisation provisions and other connected provisions in the area of computer- or computer-related crime: it first defines 9 offences grouped in 4 different categories, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

Section 2 of Chapter II (procedural law issues) - the scope of which goes beyond the offences defined in Section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form – determines first the common conditions and safeguards, applicable to all procedural powers in this Chapter. It then sets out the following procedural powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; interception of content data.

Chapter II ends with the jurisdiction provisions.

Chapter III contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer- or computer-related crime specific assistance applies to both situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Parties.
Finally, Chapter IV contains the final clauses, which - with certain exceptions - repeat the standard provisions in Council of Europe treaties.

Weakness and Criticisms:
As it is always been, nothing on earth is always perfect, and when people do constitution and conventions their must be some kind of lacks, misleading, shortage or even mistakes. In the case of Cybercrime some organization have raised criticisms, after studying their points of view I would like to show out what they pointed out, the list of these organization are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Civil Liberties Union (US)</td>
<td><a href="http://www.aclu.org/">http://www.aclu.org/</a></td>
</tr>
<tr>
<td>Associazione per la Libertà nella Comunicazione Elettronica Interattiva (IT)</td>
<td><a href="http://www.alcei.it/">http://www.alcei.it/</a></td>
</tr>
<tr>
<td>Bits of Freedom (NL)</td>
<td><a href="http://www.bof.nl/">http://www.bof.nl/</a></td>
</tr>
<tr>
<td>Center for Democracy and Technology (US)</td>
<td><a href="http://www.cdt.org/">http://www.cdt.org/</a></td>
</tr>
<tr>
<td>Digital Freedom Network (US)</td>
<td><a href="http://dfn.org">http://dfn.org</a></td>
</tr>
<tr>
<td>Electronic Frontier Foundation (US)</td>
<td><a href="http://www.eff.org/">http://www.eff.org/</a></td>
</tr>
<tr>
<td>Electronic Privacy Information Center (US)</td>
<td><a href="http://www.epic.org/">http://www.epic.org/</a></td>
</tr>
<tr>
<td>IRIS - Imagions un réseau Internet solidaire (FR)</td>
<td><a href="http://www.iris.sqdq.org/">http://www.iris.sqdq.org/</a></td>
</tr>
<tr>
<td>Kriptopolis (ES)</td>
<td><a href="http://www.kriptopolis.com/">http://www.kriptopolis.com/</a></td>
</tr>
<tr>
<td>The Link Centre, Wits University, Johannesburg (ZA)</td>
<td><a href="http://link.wits.ac.za/">http://link.wits.ac.za/</a></td>
</tr>
<tr>
<td>NetAction (US)</td>
<td><a href="http://www.netaction.org/">http://www.netaction.org/</a></td>
</tr>
<tr>
<td>Netwokers against Surveillance Taskforce (JP)</td>
<td><a href="http://www.jca.apc.org/">http://www.jca.apc.org/</a></td>
</tr>
<tr>
<td>Privacy International (UK)</td>
<td><a href="http://www.privacyinternational.org">http://www.privacyinternational.org</a></td>
</tr>
<tr>
<td>Privacy Ukraine (UA)</td>
<td><a href="http://www.ukrnet.net/">http://www.ukrnet.net/</a></td>
</tr>
<tr>
<td>quintessenz (AT)</td>
<td><a href="http://www.quintessenz.at/">http://www.quintessenz.at/</a></td>
</tr>
<tr>
<td>Verein für Internet Benutzer (AT)</td>
<td><a href="http://www.vibe.at/">http://www.vibe.at/</a></td>
</tr>
</tbody>
</table>
Exceptions indicate a larger problem

One thematic shift in the convention is the increased number of exceptions and caveats in the current draft. While, these exceptions are still quite weak, it appears as though there is rising concern within the CoE as to the powers granted within the convention.

- The effect of the deletion of Article 37.2 (from version 22), that once limited the amount of flexibility signatory states are allowed to exercise, appears as though there is an arising opposition among the drafters and plenary member states over this issue.

- In Section 2 on Investigative Techniques, article 14.2 was added to assure "adequate protection of human rights and, where applicable, the proportionality of the measures to the nature and circumstances of the offence." While the CoE considered allowing signatory states to restrict the situations for using the new investigatory powers, even from using them in the crimes established in the convention, this was not included in version 24-2. The convention still promotes use of invasive techniques for any crime, except the use of interception, which according to 21.1 can only be used for "serious offences to be determined by domestic law". Even this limitation serves little effect, for the definition of serious crime is left to domestic law, and some countries in the CoE have an extremely broad definition of serious crime for content interception purposes.

- An additional exception was appended to Articles 29 and 30, for consistency with a previous article, that a signatory state may refuse mutual assistance to pursue an offence only if the state in question considers the offence to be political. Despite that this option existed in another article in version 22, and is consistent with previous CoE documents, it does appear that the CoE is aware of the differences in regimes and qualitative nature of ‘offences’ in the prospective-signatory states. This exception arises because of the failure to require dual-criminality.

- The addition of sub-article 35(bis).4 states that a transferring party may require the receiving party to explain the use made of information that is shared between states. This after-the-fact reporting is desirable, but not sufficient. The interests of proportionality and specificity must also be addressed in requirements applicable to the initial requests for assistance, sufficient to allow the requested party to verify the reason for the investigation by the requesting party.
• When a state makes such ‘reservations’, article 43 contains new sub-articles to place pressure on these states to conform to the full powers of the convention. Sub article 43.2 claims that signatory states are expected to withdraw reservations “as soon as circumstances permit”, while sub article 43.3 allows the Secretary General to approach these states periodically to discuss the withdrawal of their reservations. The CoE appears to assume that human rights are negotiable, periodically.

Powers for Invasiveness
Power of interception and preservation of data without sufficient constraints.

• Article 19.4 continues to allow for self-incrimination by ordering an individual who has knowledge of the security methods applied to the data of interest, to provide all necessary information to enable search and seizure. Concerns remains that this may be a prompt for government access to decryption keys and could breach Article 6 of the European Convention on Human Rights.

• Article 20 on access to traffic data fails to acknowledge the invasive qualities of such data, and the shifting division between content and traffic data. Likewise, there is no definition for ‘content data’.

• The addition of article 20.2 for real-time collection and recording of traffic data through technical means appears to be a prompt to allow for systems such as Carnivore.

• The addition of article 21.2 allows similarly for "real-time collection and recording of content data through technical means."

Accession without Rights
It has been stated that the signing of this convention is intended to eventually include non-member states of the Council of Europe. It is our hope that any state that is invited to sign this convention have sufficient respect for human rights and democratic accountability. In particular, these invited states are not signatories to the European Convention on Human Rights and have not necessarily enacted into national law the principles of protection of these rights. As a result, consider this invitation to be an attack on the integrity of the convention. Required at the very least to see in Article 37 a sufficient requirement and evaluation to the adequacy of human rights protection prior to allowing their accession.

Un-due Extraterritoriality
The convention contains numerous extraterritoriality claims, particularly embodied within two statements.

• Article 23 creates supra-national reach for signatory states. Although there is an exception under sub article 23.2, which the US admits that it will have to pursue,
as we have stated earlier, if an exception exists, it is often because the measure is too far-reaching.

- Footnote 29, which relates to mutual assistance under article 27, specifies "that the mere fact that the requested Party’s legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting Party." As a result, signatory states can be forced to act beyond their means.

**Recommendations and observations:**

The main concerns about this convention is that how much it preserves people privacy and property, on the other hand, because Internet doesn’t have any geographical boundaries there must the same apply on these kind of conventions, that means must reach into international convention to be applied in countries, a simple example of this case is that one person could be criminal in one country and fully innocent in others, United Nation could play vital role into this issue by adopting or at least dealing with this convention with its main institutes like Court of Human Rights and other divisions, some main recommendations on this convention:

- *Proportionality* is a concept that must be defined at the international level, uniformly and unilaterally agreed or by reference to the jurisprudence of the European Court of Human Rights.

- The current draft's approach of allowing for exceptions and reservations by individual countries is faulty and hazardous to human rights for it fails to set a mutually agreed upon limit to the privacy intrusions that will be within the scope of the treaty.

- urge dual criminality as a pre-requisite to all forms of mutual assistance, and these crimes must be stated explicitly.

- addition of a consistent regime of civil liberties protections in investigative powers is needed.

- clear limits to the powers involving situations where civil liberties are compromised. Particularly, we expect that invasive techniques are used only in the case of serious crimes and allow for clear prevention of self-incrimination and other inalienable rights, such as privacy and freedom of expression as outlined in the European Convention on Human Rights, the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights.

- Require *limitations* on the powers of interception and data gathering devices so as to absolutely limit the invasiveness. We recommend that 20.2 and 21.2 are replaced in favour of a protective article ensuring that if technical means are used, these means must separate out the traffic of the specific user under investigation, gather only the legally permitted amount of data, disallow tampering, and respect the shifting division between content and traffic data. If
this can not be guaranteed through independent audit, these techniques must be
deemed illegal (similar to Article 3) and no data access or sharing can occur.

- **Interception of communications** is an invasive technique often used against
dissidents and human rights workers around the world. We continue to urge you
not to establish this requirement in a modern communication network particularly
as these networks are still being developed and shaped.

In increasing powers the convention must also establish a maximum threshold of
investigative techniques that are acceptable; injudicious access and data warehousing are
gross invasions of civil liberties.. Recommend a clause be included under mutual
assistance that states that when Party A requests assistance from Party B, Party B may
not act using powers greater than those allowed for under Party A's jurisdiction, and
Party B can only act based on the rule of law within Party B under due process.

**References documents and notes:**
Management of Information System , Velidamir Zwass , Fairleigh Dickinson Univesity ,
New Jersey , 1997, USA.

* Implementation of Recommendation N° R (89) 9 on computer-related crime, Report
prepared by Professor Dr. H.W.K. Kaspersen (doc. CDPC (97) 5 and PC-CY (97) 5,
page 106).

** Computer-related crime, Report by the European Committee on Crime Problems,
page 86.

*** Problems of criminal procedural law connected with information technology,
Recommendation N° R (95) 13, principle n° 17

COE Convention on Cyber-Crime (draft ver 24-2)
[http://conventions.coe.int/treaty/EN/projets/cybercrime24.htm](http://conventions.coe.int/treaty/EN/projets/cybercrime24.htm)

COE Convention for the Protection of Human Rights and Fundamental Freedoms
[http://www.coe.fr/eng/legaltxt/5e.htm](http://www.coe.fr/eng/legaltxt/5e.htm)

COE Conventions - Background
[http://conventions.coe.int/treaty/EN/cadreintro.htm](http://conventions.coe.int/treaty/EN/cadreintro.htm)

Global Internet Liberty Campaign Member Letter on Council of Europe Convention on
Cyber-Crime -- October 18 2000

Comments of the Center for Democracy and Technology on the Council of Europe Draft
"Convention on Cyber-crime" (Draft No. 24)
[http://www.cdt.org/international/cybercrime/001211cdt.shtml](http://www.cdt.org/international/cybercrime/001211cdt.shtml)
IAB/IESG Statement on Wassenaar Arrangement
http://www.iab.org/iab/121898.txt

IETF Policy on Wiretapping (RFC 2804)
ftp://ftp.isi.edu/in-notes/rfc2804.txt

IRIS Dossier cybercriminalité
http://www.iris.sgdg.org/actions/cybercrime/

http://www.oecd.org//dsti/sti/it/secu/production/e-crypto.htm

OECD Guidelines for the Security of Information

Privacy International Cyber-Crime Page
http://www.privacyinternational.org/issues/cybercrime/

Statement of Concern from Technology Professionals on Proposed COE Convention on Cyber-Crime
http://www.cerias.purdue.edu/homes/spaf/coe/TREATY_LETTER.html

Universal Declaration of Human Rights
http://dfn.org/voices/intl/udhr.htm