

2000



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 2 October 2000

Public version - Declassified
PC-CY (2000) Draft N° 22 REV 2

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE
(PC-CY)

Draft Convention on Cyber-crime
(Draft N° 22 REV.)

Prepared by the Secretariat
Directorate General I (Legal Affairs)

DRAFT CONVENTION ON CYBER-CRIME
(Draft N° 22 REV.)

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States signatories to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against *cyber-crime*, *inter alia* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at 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;

Believing that an effective fight against cyber-crime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation, while ensuring a proper balance between the interests of law enforcement and respect for fundamental human rights;

Mindful of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the 1966 United Nations International Covenant on Civil and Political Rights which both reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the right to respect for privacy;

Considering the Optional Protocol to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography as well as the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of electronic evidence of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating *cyber-crimes*, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° 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, Recommendation N° R (88) 2 on piracy in the field of copyright and neighbouring rights as well as Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (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 to 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 ;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe, on the occasion of their Second Summit (Strasbourg, 10 - 11 October 1997), to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I - Use of terms

Article 1 - Definitions¹

For the purposes of this Convention:

- a. "computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data [or any other function]²;
- b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
- c. "service provider" means:
 - i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
 - ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
- d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by the computer system that formed part in the chain of communication, indicating its origin, destination, path or route, time, date, size, duration or type of underlying [network] service.
- e. "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its service, other than traffic or content data, by which can be established:
 - i. the type of the communication service and equipment used by the subscriber and the technical provisions taken thereto;
 - ii. the subscriber's identity, address, telephone number, or any other information related to *[the subscriber or]* the location of his/her communication equipment.

¹ These definitions (1/a – 1/e) still need to be revised by the Drafting Group.

² The explanatory report should specify that "computer system" refers to the function of data processing and therefore may include any system that is based on such a function, e.g. telecom systems, and that the "inter-connection" referred to in the definition encompasses radio and logical connections.

Chapter II - Measures to be taken at the national level

Section 1 - Substantive criminal law

Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 - Illegal Access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally³ the access to the whole or any part of a computer system without right⁴. A Party may require that the offence be committed either by infringing security measures or with the intent of obtaining computer data or other dishonest intent.

Article 3 - Illegal Interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the interception without right, made by technical means, of non-public⁵ transmissions of computer data to, from or within a computer system, as well as electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent⁶.

Article 4 - Data Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the damaging, deletion, deterioration, alteration⁷ or suppression⁸ of computer data without right.

³ The interpretation of "intent" should be left to domestic laws, but it should not, where possible, exclude "*dolus eventualis*".

⁴ The expression 'without right' appears in all of the articles of this section and derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their national law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under national law.

⁵ The terms "non-public" relate to the transmission (communication) process and not necessarily to the data transmitted.

⁶ In some countries, interception may be closely related to the offence of unauthorised access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent with respect to the offence in article 2 may also require a similar qualifier to attach criminal liability to conduct defined under Article 3.

⁷ The Explanatory Report should specify that 'Alteration' also includes tampering with traffic data (spoofing).

Article 5 - System Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the serious hindering without right of the functioning of a computer system by inputting, [transmitting,] damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Illegal Devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right⁹:

- a) the production, sale, procurement for use, import, distribution or otherwise making available of:
 1. a device, including a computer program, designed or adapted [specifically] [primarily] [particularly] for the purpose of committing any of the offences established in accordance with Article 2 – 5;
 2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing the offences established in Articles 2 - 5;

- b) the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing the offenses established in Articles 2 – 5. A party may require by law that a number of such items be possessed before criminal liability attaches.

⁸ The Explanatory Report should clarify that “suppression of data” has two commonly agreed meanings: 1) delete data so that it does no longer exist physically; 2) “render inaccessible”, i.e. prevent someone from gaining access to it while maintaining it.

⁹ Several comments from industry indicated that the so-called “cracking-devices”, to which Article 6 applies, may also be used legitimately to test system security. The explanatory report shall clarify that the conduct defined by Article 6, when undertaken with such legitimate purposes, would be considered to be “with right”. Furthermore, the burden of proof of the unlawfulness of conduct under Article 6 would lie with the prosecution. In this context, reference should be made to the footnote under Article 2 concerning the meaning of “without right”.

Title 2 - Computer-related offences

Article 7 – Computer-related Forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic¹⁰, regardless whether or not the data is directly readable and intelligible. A Party may require by law an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related Fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing, without right, of a loss of property to another by:

- a) any input, alteration, deletion or suppression of computer data,
- b) any interference with the functioning of a computer [program] or system,

with the intent of procuring, without right, an economic benefit for himself or for another.

Title 3 - Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed without right¹¹ and intentionally the following conduct:

- a. offering¹² or making available child pornography through a computer system;
- b. distributing or transmitting child pornography through a computer system;
- c. producing child pornography for the purpose of its distribution through a computer system¹³;

¹⁰ The Explanatory Report shall specify that the term “authentic” refers to the issuer of the data, regardless whether the content of the data is true or not.

¹¹ The Explanatory Report should clarify that the terms “without right” do not exclude legal defenses, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Therefore, conduct undertaken with artistic, medical or similar scientific purposes would not be “without right”.

¹² The Explanatory Report should specify that ‘offering’ also includes giving information about hyperlinks to child-pornography sites and that “making available” is, for example, posting child pornography on the internet or making it available through file sharing technologies.

¹³ The Explanatory Report should clarify that this provision by no means is intended to restrict the criminalisation of the distribution, etc, of child pornography to cases making use of a computer system, but the Convention establishes this only as a minimum standard and States are free to go beyond it.

- d. possessing child pornography in a computer system or on a computer-data storage medium.
2. For the purpose of paragraph 1 above “child pornography” shall include pornographic material¹⁴ that visually depicts:
 - a. a minor engaged in a sexually explicit conduct¹⁵;
 - b. a person appearing to be a minor engaged in a sexually explicit conduct;
 - c. realistic images representing a minor engaged in a sexually explicit conduct.
 3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 - Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Berne Convention for the Protection of Literary and Artistic Works the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed intentionally¹⁶, on a commercial scale¹⁷ and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights

¹⁴ The Explanatory Report should clarify that the term “pornographic material” is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt.

¹⁵ The Explanatory Report should specify that a “sexually explicit conduct” covers at least actual or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse; or e) lascivious exhibition of the genitals or the pubic area of a minor.

¹⁶ Some delegations preferred to use the word “willfully” instead of “intentionally” in both paragraphs 1 and 2, on the ground that “willfully” is used in article 61 of the TRIPS agreement (governing obligation to criminalise) and in some legal systems connotes a specific intent to infringe a copyright on a commercial scale.

¹⁷ There are still discussions concerning criteria that would allow Parties to exclude minor offences from the scope of this provision.

and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed intentionally, on a commercial scale and by means of a computer system.

Title 5 – Ancillary liability and sanctions

Article 11 - Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1)b and 9(1)c of this Convention.
3. Each State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to apply, in part or in whole paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for the criminal offences established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:
 - a power of representation of the legal person; or
 - an authority to take decisions on behalf of the legal person; or
 - an authority to exercise control within the legal person;
 - as well as for involvement of such a natural person as aidor or abettor, under Article 11, in the above-mentioned offences.
2. Apart from the cases already provided for in paragraph 1, each Party shall take the necessary measures to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of the criminal offences mentioned in paragraph 1 for the benefit of that legal person by a natural person under its authority.
3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators, aidors or abettors of the criminal offences mentioned in paragraph 1.

Article 13 – Sanctions and measures

1. Each Party shall take the necessary measures to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Section 2 – Procedural law

Article 14 - Search and Seizure of Stored Computer Data

1. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
 - a) a computer system or part of it and computer data stored therein; or
 - b) a computer-data storage medium in which computer data may be stored

in its territory for the purposes of criminal investigations or proceedings.

2. Each Party shall take such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, using the measures referred to in paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2 in view of their possible use in criminal investigations or proceedings. These measures shall include the power to :
 - a. seize or similarly secure a computer system or part of it or a computer-data storage medium;
 - b. make and retain a copy of those computer data;
 - c. maintain the integrity of the relevant stored computer data;
 - d. render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to order for the purposes of criminal investigations or proceedings any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide all necessary information, as is reasonable, to enable the undertaking of the measures referred to in paragraphs 1 and 4.

5. [Where measures referred to in paragraphs 1 and 2 have been taken in respect of a computer system or part of it, or computer data stored therein, the custodian of the system or of the storage medium¹⁸ shall, when reasonably practicable, be duly informed about the executed measures.]

Article 15 - Production Order

Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to order, for the purpose of criminal investigations or proceedings:

- a) a person in its territory to submit¹⁹ specified computer data under this person's control, which is stored in a computer system or a computer-data storage medium;
- b) a service provider offering its services in its territory to submit subscriber information under that service provider's possession or control;
- c) [Option 1: a person in its territory to process specified computer data under this person's control in order to yield the information necessary for that purpose and submit it to the competent authorities] [Option 2: a person in its territory to produce, within that person's technical ability, specified information by processing data under that person's possession or control].²⁰

Article 16 – Expedited preservation of data stored in a computer system

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or otherwise obtain, for the purpose of criminal investigations or proceedings, the expeditious preservation of data that is stored by means of a computer system, at least where there are grounds to believe that the data is subject to a short period of retention or is otherwise particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that data for a period of time as may be ordered pursuant to domestic law.

¹⁸ The Explanatory Report shall clarify that this provision refers to persons having an actual (physical) control over the computer (system). This would normally include the owner of the premises where the computer is located or the owner/user of the computer itself.

¹⁹ A Party may, by implementing this power in domestic law, require additional criteria and/or conditions, such as "in the manner specified in the order".

²⁰ Paragraph 1/c is still under discussion. It would allow to oblige private persons to process data for law enforcement purposes, e.g. analyse them according to certain criteria relevant for law enforcement or apply to them "data-matching" techniques for these purposes. It may look like being a far-reaching, intrusive power, but it could offer more guarantees for the protection of private life than it seems. If a private person applies "data-matching", only the result will be available for the law enforcement authorities. Without such an obligation, it might be necessary that these authorities obtain vast amounts of data or complete files – e.g. through the power provided for under article 15 - in order to do "data-matching" themselves.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige a person to whom the procedures of preservation referred to in this Article are directed, to keep confidential the undertaking of such procedures for a period of time as permitted by domestic law.

Article 17 – Expedited preservation and disclosure of traffic data

Each Party shall, with respect to undertaking the procedures referred to under article 16 in respect of the preservation of traffic data concerning a specific communication, adopt such legislative or other measures as may be necessary to:

- a) ensure the expeditious preservation of that traffic data, regardless whether one or more service providers were involved in the transmission of that communication; and
- b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data in order to identify the service providers and the path through which the communication was transmitted.

Article 18 - Interception of electronic communications

Each Party shall take such legislative and other measures as may be necessary, for the purpose of criminal investigations or proceedings related to serious offences [to be defined by domestic law] to empower its competent authorities to:

- (a) collect or record through application of technical means on the territory of that Party, and
- (b) compel a service provider to:
 - (i) collect or record through application of technical means on the territory of that Party, or
 - (ii) co-operate and assist the competent authorities in the collection or recording of,

content data of specified communications in its territory²¹ transmitted by means of a computer system.

Article 18 bis - Real-time collection of traffic data

Each Party shall take such legislative and other measures as may be necessary, for the purpose of criminal investigations or proceedings, to empower its competent authorities to:

²¹ The Explanatory Memorandum shall clarify that there is a communication on a country's territory if one of the communicating parties (human beings or computers) is located there.

- (a) collect or record through application of technical means on the territory of that Party and
- (b) compel a service provider to:
 - (i) collect or record through application of technical means on the territory of that Party, or
 - (ii) co-operate and assist the competent authorities in the collection or recording of,

traffic data in real-time, associated with specified communications on its territory transmitted by means of a computer system.

Article 18 ter – Obligation of confidentiality

Each Party shall take such legislative and 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 power provided for under Articles 18 and 18 bis.

Article 18 quater - General Provisions Relating to Domestic Procedural Law Measures

1. [Each Party shall apply the measures described in articles 14 through 17, and 18 bis to:
 - (a) the offences established in accordance with articles 2-11 of this Convention;
 - (b) other criminal offences committed by means of a computer system;
 - (c) evidence in electronic form of any criminal offence.]
2. [Each Party may, at the time of signature, or when depositing its instruments of ratification, acceptance, approval or accession, by declaration addressed to the Secretary General of the Council of Europe, declare that it reserves its right to apply the measure referred to in Article 18 bis only to offences or categories of offences specified in such declaration.]
3. For the purposes of Article 18, the range of serious offenses covered shall be determined by the domestic law of the Party concerned.
4. The powers and procedures referred to in articles 14 through 18 bis shall be subject to the conditions²² and safeguards provided for under the domestic law of the Party concerned.

²² The terms “conditions and safeguards” refer to procedural modalities of the powers defined in Articles 14 through 18bis. The Explanatory Report shall provide some examples of the kinds of conditions and safeguards, which Parties may wish to require.

Section 3 - Jurisdiction

Article 19 - Jurisdiction

1. Each Party shall take such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 – 11 of this Convention, when the offence is committed
 - a) in its territory; or
 - b) on board a ship flying the flag of that Party; or
 - c) on board an aircraft registered under the laws of that Party; or
 - d) on board a satellite²³ [registered in ...]; or
 - e) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) e of this article or any part thereof.
3. If a Party has made use of the reservation possibility provided for in paragraph 2 of this article, it shall adopt such measures as may be necessary to establish jurisdiction over a criminal offence referred to in Article 21, paragraph 1 of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him to another Party, solely on the basis of his nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

²³ Further clarification is required with regard to the inclusion of satellites, in particular as to whether this provision would require a State that has responsibility for a satellite (or shares such responsibility with other States) to establish jurisdiction over an offence where the only nexus with that State is that data related to the offence has been transmitted through that satellite. Other international instruments should be examined to determine how they affect the jurisdiction of States with respect to satellites. The way of registration for satellites and the reference to the State entering such registration should also be clarified.

Chapter III – International Co-operation

Section 1 – General principles

Article 20 - General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.

Section 2 - Extradition

Article 21 - Extradition

1. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. Where an extradition treaty or arrangement agreed on the basis of uniform or reciprocal legislation is in force between two or more Parties, which requires a different minimum penalty for extradition, the minimum penalty provided for in such treaty or arrangement shall instead apply.
2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this Article.
4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this Article as extraditable offences between themselves.
5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this Article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that State.
7. (a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority²⁴ responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

(b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Section 3 – Mutual assistance

Article 22 – General principles related to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.
2. Each Party shall also adopt such legislative or other measures as may be necessary to carry out the obligations set forth in Articles 24 - 29.
3. For the purpose of providing cooperation under articles 24 - 29, each Party shall, in urgent circumstances, accept and respond to mutual assistance requests by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication, with formal confirmation to follow where required by the requested State.

²⁴ Designation of an authority shall not exclude the possibility of using the diplomatic channel. This provision has been limited to situations in which there is no extradition treaty in force between the Parties concerned. Where a bilateral or multilateral extradition treaty is in force between the Parties concerned (such as the 1957 European Convention on Extradition), the Parties will know to whom extradition and provisional arrest requests are to be directed without the necessity of a burdensome registration requirement.

4. Except as otherwise specifically provided in Articles 24 – [29]²⁵, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse cooperation.
5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 23 - Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation, in force between the requesting and requested Parties, the provisions of paragraphs 2 through 10 of this article shall apply. The provisions of this article shall not apply where such agreement, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this Article in lieu thereof.
2. (a) Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.

(b) The central authorities shall communicate directly with each other.

(c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

(d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.²⁶

²⁵ It is still under discussion whether the condition of dual criminality should be required for certain procedural measures (expedited preservation of stored computer data – Article 24 – and expedited disclosure of preserved traffic data – Article 25) as a matter of principle.

²⁶ The explanatory text should specify 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.

4. The requested Party may, in addition to conditions or grounds for refusal available under Article 22 (4), refuse assistance:
 - a) if the request concerns an offences which the requested Party considers a political offence or an offence connected with a political offence;
 - b) if it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
5. The requested Party may postpone action on a request if such action would prejudice investigations, prosecutions or related proceedings by its authorities.
6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
8. (a) Without prejudice to its own investigations or proceedings, a Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for cooperation by that Party under this chapter.

(b) Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.
9. (a) The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

(b) The requesting Party may request that the requested Party not, without the prior consent of the requesting Party, make use of the substance of the request, [nor of the information obtained pursuant to having executed the request,] for purposes other than those for which it was obtained or for criminal investigations and related proceedings. If the requested Party cannot comply with the request, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

(c) The requested Party may request that the requesting Party not, without the prior consent of the requested Party, transmit or use the materials furnished for investigations or proceedings other than those stated in the request. If the requesting Party accepts the materials subject to the conditions, it shall be bound by them. If the requesting Party cannot comply with the conditions, it shall promptly inform the requested Party, which shall then determine whether the materials should nevertheless be provided.

10. (a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

(b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

(c) Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

(d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

(e) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Section 4 – Mutual assistance regarding provisional measures

Article 24 - Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2. A request for preservation made under paragraph 1 shall specify:
 - a) the authority that is seeking the preservation;
 - b) the offence under investigation and a brief summary of related facts;
 - c) the stored data to be preserved and its relationship to the offence;
 - d) the necessity of the preservation;

- e) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required²⁷ as a condition to providing such preservation, but may be required as a condition for the disclosure of the data to the requesting Party.
 4. A request for preservation as described in paragraph 2 may only be refused if the requested Party believes that compliance with the request would prejudice its sovereignty, security, *ordre public* or other essential interests.
 5. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
 6. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 40 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 25 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 24 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in a third State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 may only be withheld if the requested Party believes that compliance with the request would prejudice its sovereignty, security, *ordre public* or other essential interests.

Section 5 – Mutual assistance regarding [coercive] [investigative] powers

Article 26 - Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 24.

²⁷ Further consideration is necessary on this matter, given that certain delegations expressed reservations as to the possibility of giving up the requirement of dual criminality.

2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in article 20, and in accordance with other relevant provisions of this Chapter.
3. For the purpose of expediting the execution of the request under this Article, each Party [shall] [may], subject to its domestic law, ratify or endorse a judicial or other legal authorisation granted in another Party to search or similarly access or seize or similarly secure the data. Disclosure of the data shall be governed by the instruments, arrangements and laws referred to in paragraph 2.
4. The request shall be responded to on an expedited basis where:
 - a. there are grounds to believe that relevant data is subject to a short period of retention, or is otherwise particularly vulnerable to loss or modification; or
 - b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 27 - Transborder access to stored computer data not requiring mutual legal assistance

1. A Party may, without obtaining the authorisation of another Party:
 - a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
 - b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[2. Under discussion]

Article 28 – Mutual assistance regarding the interception of data

The Parties shall provide mutual assistance to each other with respect to the interception of the content of specified communications transmitted by means of a computer system [to the extent permitted by their applicable treaties and domestic laws].

Article 28 bis - Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data concerning specified communications transmitted by means of a computer system. Subject to subparagraph 3, assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to [the offences established in accordance with this convention and such other] [the offences established in accordance with articles 2 through 5 and 9 of this convention and such other] criminal offences for which real-time collection would be available in a similar national case.
3. Parties that limit the types of offences for which the measure is available shall consider expanding their ability to provide such assistance to other criminal offences related to computer systems and data.

Section 6 – 24/7 Network

Article 29 - 24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of the investigation of criminal offenses related to the use of computer systems and data, or for the collection of electronic evidence of any criminal offense. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:
 - (1) providing technical advice;
 - (2) preservation of data pursuant to Articles 24 and 25; and
 - (3) the collection of evidence, giving of legal information, and locating of suspects.
2. (a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

(b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis.
3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Chapter V – Follow-up

[Articles 30 – 32 – Follow-up]

Under discussion

Chapter VI – Final Provisions

Article 33 – Signature and entry into force

1. This convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration. Such States may express their consent to be bound by:
 - a signature without reservation as to ratification, acceptance or approval; or
 - b signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.
2. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which States have expressed their consent to be bound by the Convention in accordance with the provisions of paragraph 1.
4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of their consent to be bound by the Convention in accordance with the provisions of paragraph 1.

Article 34 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting the Contracting States to the Convention, may invite the European Community as well as any State not a member of the Council and not having participated in its elaboration to accede to this Convention, by a decision taken by the majority provided for in Article 20d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
2. In respect of the European Community and any State acceding to it under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 35 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
2. Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory

specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declarations by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 36 – Relationship to other conventions and agreements

1. *[Under discussion]*
2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise have established their relations in this matter, or should they in future do so, they shall be entitled to apply that agreement or treaty or to regulate those relations accordingly, in lieu of the present Convention.

Article 37 – Declarations

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the declaration provided for under [Articles ...]
2. No State may, by application of paragraph 1 of this article, make a declaration with respect to more than [...] of the provisions mentioned thereon. No other declaration may be made. Declarations of the same nature with respect to [Articles .. and ..] shall be considered as one declaration.
3. A Party that is a federal State shall be required to assume obligations under this Convention only to the extent consistent with its constitutional principles governing the relationship between its central government and other constituent units.

Article 38 – Reservations

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession declare that it avails itself of the reservation provided for in [Articles ...]
2. No State may, by application of paragraph 1 of this article, enter reservations to more than [...] of the provisions mentioned thereon. No other reservation may be made.

Article 39 – Validity and review of declarations and reservations

- [1. Declarations as referred to in Article 37 and reservations as referred to in Article 38 shall be valid for a period for three years from the day of the entry into force of this Convention in respect of the State concerned. However, such declarations and reservations may be renewed for periods of the same duration.

2. Twelve months before the date of expiry of the declaration or reservation, the Secretariat General of the Council of Europe shall give notice of that expiry to the State concerned. No later than three months before the expiry, the State shall notify the Secretary General that it is upholding, amending or withdrawing its declaration or reservation. In the absence of a notification by the State concerned, the Secretariat General shall inform that State that its declaration or reservation is considered to have been extended automatically for a period of six months. Failure by the State concerned to notify its intention to uphold or modify its declaration or reservation before the expiry of that period shall cause the declaration or reservation to lapse.
3. If a Party makes a declaration in conformity with Article 37 or a reservation in conformity with Article 38, it shall provide, before its renewal or upon request, an explanation to , on the grounds justifying its continuance.]

[Article 40 — Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to, or has been invited to accede to this Convention in accordance with the provisions of Article 34.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation of the non-member State Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.]

[Article 41 – Settlement of disputes

1 The European Committee on Crime Problems of the Council of Europe shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.]

Article 42 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 43 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe and any State which has acceded to this Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;
- c any date of entry into force of this Convention in accordance with Articles 33 and 34;
- d any declaration or reservation made under Article 37 or Article 38;
- e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, on 200?, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.