108TH CONGRESS
1st Session

SENATE

TREATY DOC.
108–11

CONVENTION ON CYBERCRIME

MESSAGE

FROM

THE PRESIDENT OF THE UNITED STATES

TRANSMITTING

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (THE "CYBERCRIME CONVENTION" OR THE "CONVENTION"), WHICH WAS SIGNED BY THE UNITED STATES ON NOVEMBER 23, 2001

NOVEMBER 17, 2003.—Convention was read the first time, and together with the accompanying papers, referred to the Committee on Foreign Relations and ordered to be printed for the use of the Senate

U.S. GOVERNMENT PRINTING OFFICE

29–118 WASHINGTON : 2003

LETTER OF TRANSMITTAL

THE WHITE HOUSE,
November 17, 2003.

To the Senate of the United States:

With a view to receiving the advice and consent of the Senate to ratification, I transmit herewith the Council of Europe Convention on Cybercrime (the "Cybercrime Convention" or the "Convention"), which was signed by the United States on November 23, 2001. In addition, for the information of the Senate, I transmit the report of the Department of State with respect to the Convention and the Convention's official Explanatory Report.

The United States, in its capacity as an observer at the Council of Europe, participated actively in the elaboration of the Convention, which is the only multilateral treaty to address the problems of computer-related crime and electronic evidence gathering. An overview of the Convention's provisions is provided in the report of the Department of State. The report also sets forth proposed reservations and declarations that would be deposited by the United States with its instrument of ratification. With these reservations and declarations, the Convention would not require implementing legislation for the United States.

The Convention promises to be an effective tool in the global effort to combat computer-related crime. It requires Parties to criminalize, if they have not already done so, certain conduct that is committed through, against, or related to computer systems. Such substantive crime include offenses against the "confidentiality, integrity and availability" of computer data and systems, as well as using computer systems to engage in conduct that would be criminal if committed outside the cyber-realm, i.e., forgery, fraud, child pornography, and certain copyright-related offenses. The Convention also requires Parties to have the ability to investigate computer-related crime effectively and to obtain electronic evidence in all types of criminal investigations and proceedings.

By providing for broad international cooperation in the form of extradition and mutual legal assistance, the Cybercrime Convention would remove or minimize legal obstacles to international cooperation that delay or endanger U.S. investigations and prosecutions of computer-related crime. As such, it would help deny "safe havens" to criminals, including terrorists, who can cause damage to U.S. interests from abroad using computer systems. At the same time, the Convention contains safeguards that protect civil liberties and other legitimate interests.

I recommend that the Senate give early and favorable consideration to the Cybercrime Convention, and that it give its advice and consent to ratification, subject to the reservations, declarations,

and understanding described in the accompanying report of the Department of State.

GEORGE W. BUSH.

LETTER OF SUBMITTAL

DEPARTMENT OF STATE,
Washington, September 11, 2003.

The PRESIDENT,
The White House.

THE PRESIDENT: I have the honor to submit to you, with a view to its transmittal to the Senate for advice and consent to ratification, the Council of Europe ("COE") Convention on Cybercrime ("the Cybercrime Convention" or "the Convention"), which was adopted by the COE's Committee of Ministers on November 8, 2001. On November 23, 2001, the United States, which actively participated in the negotiations in its capacity as an observer state at the COE, signed the Convention at Budapest. I recommend that the Convention be transmitted to the Senate for its advice and consent to ratification.

Accompanying the Convention is its official Explanatory Report, which was also adopted by the COE's Committee of Ministers on November 8, 2001. The Explanatory Report, which was drafted by the Secretariat of the COE and the delegations participating in the negotiations, provides a thorough analysis of the Convention. It is customary for the COE to prepare such reports in connection with its conventions. Under established COE practice, such reports reflect the understanding of the Parties in drafting convention provisions and, as such, are accepted as fundamental bases for interpretation of COE conventions. The Explanatory Report would be provided to the Senate for its information.

The Cybercrime Convention is the first multilateral treaty to address specifically the problem of computer-related crime and electronic evidence gathering. With the growth of the Internet, attacks on computer networks have caused large economic losses and created great risks for critical infrastructure systems. Examples of such cybercrime activities include the deliberate transmission of "viruses," "denial of service" attacks, and "hacking" into government and financial institution computer systems. Criminals around the world are also using computers to commit traditional crimes, such as fraud, child pornography and copyright piracy. In addition, computer networks provide organized crime syndicates and terrorists means with which to plan, support, coordinate, and commit their criminal activities.

In response to this growing problem of computer-related crime, the COE established in 1997 the Committee of Experts on Crime in Cyber-space ("PC–CY") to undertake negotiation of the Cybercrime Convention. States participating in the work of the PC–CY included the United States, COE member states, Canada, Japan, and South Africa. Beginning in April 2000, drafts of the

Convention were made public by the COE, so that interested members of the public could review and provide comments to the PC–CY. In addition, U.S. Government officials sought to make information about the Convention available to interested members of the public. Since its adoption, 37 states have signed the Convention, including three COE member states that have also ratified it.

The Convention establishes a treaty-based framework that requires Parties to criminalize certain conduct related to computer systems and to ensure that certain investigative procedures are available to enable their domestic law enforcement authorities to investigate cybercrime offenses effectively and obtain electronic evidence (such as computer data) of crime. In a manner analogous to other law enforcement treaties to which the United States is a party, the Convention also requires Parties to provide broad international cooperation in investigating computer-related crime and obtaining electronic evidence.

By requiring Parties to establish certain substantive offenses, the Convention will help deny "safe havens" to criminals, including terrorists, who can cause damage to U.S. interests from abroad using computer systems. Similarly, by requiring Parties to have certain procedural authorities, the Convention will enhance the ability of foreign law enforcement authorities to investigate crimes effectively and expeditiously, including those committed by local criminals against U.S. individuals, institutions and interests. Since cybercrimes are often committed via transmissions routed through foreign Internet Service Providers ("ISPs") and criminals increasingly seek to hide evidence of their crimes abroad, the Convention would also provide mechanisms for U.S. law enforcement authorities to work cooperatively with their foreign counterparts to trace the source of a computer attack and to obtain electronic evidence stored outside the United States. Thus, the Convention's obligations on Parties to establish domestic law enforcement frameworks and create a regime of international cooperation would enhance the United States' ability to receive, as well as render, international cooperation in preventing, investigating and prosecuting computer-related crime.

The Convention would not require implementing legislation for the United States. As discussed below, existing U.S. federal law, coupled with six reservations and four declarations, would be adequate to satisfy the Convention's requirements for legislation. All of these reservations and declarations are envisaged by the Convention itself. Since other provisions contained in the Convention are self-executing (e.g., articles relating to extradition and mutual assistance), they would not require implementing legislation either.

The Cybercrime Convention consists of 48 articles divided among four chapters: (1) "Use of terms"; (2) "Measures to be taken at the national level"; (3) "International co-operation"; and (4) "Final provisions." A detailed, article-by-article analysis is contained in the accompanying Explanatory Report. In addition, the following is an overview of the major Convention obligations and a description of the proposed reservations, declarations, and understanding.

CHAPTER I—USE OF TERMS (ARTICLE 1)

Chapter I, Article 1, contains definitions of four key terms that are used throughout the Convention: "computer system," "computer data," "service provider," and "traffic data." "[C]omputer system" is defined to mean any device or group of inter-connected or related devices, where one or more of them performs automatic processing of data pursuant to a program. As elaborated upon in the Explanatory Report (paragraph 23), the Convention's definition of "computer system" may include input, output and storage facilities and can be either a "stand alone" system or one that is networked with similar devices. The term "service provider" includes public and private entities that provide users with the ability to communicate by means of a computer system, as well as other entities that process or store computer data for such entities or users. The definition of "computer data" encompasses data in electronic or another form suitable for processing by a computer system. As defined in Article 1, "traffic data" does not relate to the content of a communication but instead is data generated by computers in a communication chain that relates to the communication's origin, destination, route, time, date, size, duration, or type of underlying service. As such, traffic data can provide information about the source of a computer-related crime as well as other evidence of the crime. The Explanatory Report (paragraph 22) explains that it is not necessary for Parties to copy verbatim these definitions into their laws provided the concepts are covered, as they are under existing U.S. domestic law.

CHAPTER II—MEASURES TO BE TAKEN AT THE NATIONAL LEVEL (ARTICLES 2–22)

Chapter II consists of three parts, covering substantive criminal offenses that Parties are to establish; procedural mechanisms that Parties must have under their respective laws; and provisions requiring Parties to establish jurisdiction over the offences to be established. As discussed further in connection with Article 41 ("Federal clause"), a federal state may reserve the right to assume obligations under Chapter II "consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities." In explaining this provision, the Explanatory Report (paragraph 317) makes clear that the United States could therefore implement its obligations under Chapter II through its federal criminal law, which "generally regulates conduct based on its effects on interstate or foreign commerce, while matters of minimal or purely local concern are traditionally regulated by constituent States." Thus, provided it invokes the Federal clause reservation provided for in Article 41, the United States would be able to rely on its existing federal laws, which, because of the architecture of the Internet and computer networks, provide for broad coverage of the obligations contained in Chapter II. The United States would not be obligated to criminalize activity that otherwise would not merit an exercise of federal jurisdiction. Similarly, whether or not constituent State laws conform to the Convention would not be an issue since the United States, having invoked the federal clause reservation, would

not be required to implement the Convention's obligations at that level.

Substantive criminal law (Articles 2–13):

Articles 2–10 of the Convention require Parties to criminalize domestically, if they have not already done so, certain conduct that is committed through, against or related to computer systems. Included in these substantive crimes are the following offenses against the "confidentiality, integrity and availability" of computer data and systems: "Illegal access" (Article 2), "Illegal interception" (Article 3), "Data interference" (Article 4), "System interference" (Article 5), and "Misuse of devices" (Article 6). Also included are offenses involving the use of computer systems to engage in conduct that is presently criminalized outside the cyber-realm, i.e., "Computerrelated forgery" (Article 7), "Computer-related fraud" (Article 8), "Offences related to child pornography" (Article 9), and "Offences related to infringements of copyright and related rights" (Article 10).

For criminal liability to attach under the offenses to be established pursuant to Articles 2–10, the conduct in question must be committed intentionally. As the Explanatory Report (paragraph 113) notes, "wilfully" was used in lieu of "intentionally" in the context of Article 10 infringements so as to conform with Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"), which employs the term "wilful." In addition, the Report (paragraph 39) explains that determinations of what constitutes the necessary criminal intent are left to each Party's interpretation under its laws.

The obligation to establish offenses under the Convention extends only to acts committed "without right." This concept recognizes that in certain instances conduct may be legal or justified by established legal defenses, such as consent, or by other principles or interests that preclude criminal liability. Thus, as explained in the Explanatory Report (paragraph 38), the Convention does not require the criminalization of actions undertaken pursuant to lawful government authority (e.g., steps taken by a Party's government to investigate criminal offenses or to protect national security). Additional guidance regarding the contours of "without right" is provided in the Explanatory Report (e.g., paragraphs 43, 47, 48, 58, 62, 68, 76, 77, 89, 103) in the context of the various offenses to be established. Such guidance makes it clear that authorized transmissions, legitimate and common activities inherent in the design of computer networks, and legitimate and common operating or commercial practices should not be criminalized. The condition that conduct be committed "without right" is explicitly stated in all but one of the enumerated offenses. The one exception is Article 10 ("Offences related to infringement of copyright and related rights"), where it was determined that the term "infringement" already captured the concept of "without right" (Explanatory Report, paragraph 115).

The requisite elements for the various offenses are set forth in Articles 2–10. Except for Article 5 ("System interference") and Article 8 ("Computer-related fraud"), these articles also provide that a Party may require certain additional criminalization elements or

may otherwise limit application of a criminalization obligation, provided a permitted declaration or reservation is made in accordance with Articles 40 and 42. This approach seeks to promote uniform application of the Convention while recognizing that permitting Parties to maintain established concepts in their domestic law will broaden acceptance of the Convention. As discussed below, in order to implement the Convention's substantive criminal law obligations under existing federal criminal law, the United States would avail itself of declarations and reservations provided for in Articles 2, 4, 6, 7, 9, 10, and 41.

In terms of the specific offenses against the confidentiality, integrity and availability of computer data and systems, Article 2 ("Illegal access") requires a Party to criminalize unauthorized intrusions into computer systems (often referred to as "hacking," "cracking" or "computer trespass"). Such intrusions can result in damage to computer systems and data, and compromise the confidentiality of data. Under Article 2, a Party may require certain additional elements for there to be criminal liability, including that the offense must be committed with an intent to obtain computer data. In order to correspond with the requirement contained in existing U.S. computer crime law, 18 U.S.C. § 1030(a)(2) & (b), I recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of the United States of America declares, pursuant to Articles 2 and 40, that under United States law, the offense set forth in Article 2 ("Illegal access") includes an additional requirement of intent to obtain computer data.

Article 3 ("Illegal interception") seeks to protect the privacy of non-public computer data transmissions from activities such as monitoring and recording through technical means (Explanatory Report, paragraph 54).

Article 4 ("Data interference") requires a Party to criminalize "the damaging, deletion, deterioration, alteration or suppression of computer data," which the Explanatory Report (paragraphs 60 and 61) makes clear would include the inputting of malicious codes, such as viruses, that can threaten the integrity, functioning or use of computer data and programs. Under Article 4(2), a Party may reserve the right to require that such conduct result in serious harm. In order to maintain federal jurisdictional damage thresholds, e.g., 18 U.S.C. § 1030(a)(5)(B), I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 4 and 42, reserves the right to require that the conduct result in serious harm, which shall be determined in accordance with applicable United States federal law.

Article 5 ("System interference") requires a Party to criminalize acts with respect to data which seriously hinder the functioning of a computer system. Examples of such acts are provided by the Explanatory Report (paragraph 67) and include using programs to generate denial of service attacks and transmitting malicious code, such as viruses, to stop or slow the functioning of a computer system.

The offenses to be established under Articles 2–5 are frequently committed using computer programs or access tools, such as stolen

passwords or access codes. To deter their use for the purpose of committing Article 2–5 offenses, Article 6 ("Misuse of devices") requires a Party to criminalize the possession, production, sale, procurement for use, import, distribution, or making available of such items. As recognized in the Explanatory Report (paragraph 73), however, devices such as computer programs can be used for either criminal or non-criminal purposes (so-called "dual use" devices). To avoid criminalizing activities related to devices intended for legitimate purposes, the Article provides that devices must be "designed or adapted primarily for the purpose of committing" an Article 2–5 offense. Moreover, Article 6 provides that activities in relation to devices, passwords or access codes, including their production and distribution, must be done with the intent that such devices, passwords or access codes be used for the purpose of committing an Article 2–5 offense. The Article also makes clear that it "shall not be interpreted" to impose criminal liability on the authorized testing or protection of a computer system.

With respect to the possession offense, Article 6(1)(b) provides that a Party may require that a number of items be possessed before criminal liability attaches. United States law, 18 U.S.C. § 1029(a)(3), requires that a person possess fifteen or more access devices in order for there to be federal jurisdiction. I therefore recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of the United States of America declares, pursuant to Articles 6 and 40, that under United States law, the offense set forth in paragraph (1)(b) of Article 6 ("Misuse of devices") includes a requirement that a minimum number of items be possessed. The minimum number shall be the same as that provided for by applicable United States federal law.

Article 6(3) provides that a Party may reserve the right not to apply the criminalization requirement for the misuse of items, so long as the reservation does not concern the sale, distribution or making available of passwords, access codes or similar data with the intent that they be used for committing an Article 2–5 offense. United States law does not directly criminalize the possession or distribution of data interference and system interference devices. Therefore, I recommend that the United States limit its obligations accordingly by including the following reservation in its instrument of ratification:

> The Government of the United States of America, pursuant to Articles 6 and 42, reserves the right not to apply paragraph (1)(a)(i) and (1)(b) of Article 6 ("Misuse of devices") with respect to devices designed or adapted primarily for the purpose of committing the offenses established in Article 4 ("Data interference") and Article 5 ("System interference").

With respect to the substantive crimes to be established which involve the use of computer systems to commit acts that would normally be considered criminal if committed outside the cyber-realm, Article 7 ("Computer-related forgery") seeks to protect the security and reliability of data by creating an offense akin to the forgery of tangible documents. The Article requires a Party to criminalize 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 authentic, regardless of whether the data is directly readable and intelligible. It also allows a Party to require intent to defraud, or similar dishonest intent, before criminal liability attaches. In order to enable the offense to be covered under applicable U.S. fraud statutes, I recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of the United States of America declares, pursuant to Articles 7 and 40, that under United States law, the offense set forth in Article 7 ("Computer-related forgery") includes a requirement of intent to defraud.

Article 8 ("Computer-related fraud") requires a Party to criminalize manipulations of data that are done with fraudulent intent and to procure an unlawful economic benefit. As indicated in the Explanatory Report (paragraph 86), an example of an activity that would be encompassed by the Article 8 offense is the serious problem of on-line credit card fraud.

Articles 9 and 10 deal with content-related offenses. Article 9. ("Offences related to child pornography") requires a Party to criminalize various aspects of the production, possession, procurement, and distribution of child pornography through computer systems. The Explanatory Report (paragraph 93) notes that it was believed important to include Article 9 because of the increasing use of the Internet to distribute materials created through sexual exploitation of children. In addition to covering visual depictions of an actual minor engaged in sexually explicit conduct, the Article covers images of a person appearing to be a minor engaged in such conduct as well as realistic images representing a minor engaged in such conduct (so-called "virtual" child pornography). Article 9(4), however, provides that a Party may reserve the right not to criminalize cases of a person appearing to be a minor or realistic images representing a minor engaged in such conduct. These categories were covered under U.S. law by 18 U.S.C. § 2256(8)(B), (C) & (D), and to the extent that such images are obscene, certain conduct relating to such obscene images is also covered by federal obscenity law. In light of the U.S. Supreme Court's decision in *Ashcroft* v. *Free Speech Coalition*, 535 U.S. 234 (2002), ruling § 2256(8)(B) & (D) unconstitutional, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 9 and 42, reserves the right to apply paragraphs (2)(b) and (c) of Article 9 only to the extent consistent with the Constitution of the United States as interpreted by the United States and as provided for under its federal law, which includes, for example, crimes of distribution of material considered to be obscene under applicable United States standards.

Article 10 ("Offences related to infringement of copyright and related rights") is directed at infringements of intellectual property rights, i.e., copyright and related rights, by means of a computer system and on a commercial scale. Its approach differs from the other articles requiring the establishment of offenses in that it defines the offenses by reference to other international agreements, which are set forth in the Article. Specifically, a Party is required under Article 10 to establish as criminal offenses acts that are com-

mitted "wilfully, on a commercial scale and by means of a computer system" and that are defined as infringements of copyright or related rights, under its domestic law, pursuant to obligations it has undertaken in the referenced agreements. As indicated in the Explanatory Report (paragraphs 110 and 111), a Party's obligations under this Article are framed only by those agreements that have entered into force and to which it is party. Moreover, a Party's obligations under Article 10 may be limited by reservations or declarations it has made with respect to the referenced agreements. For the purpose of determining the United States' obligations under Article 10, the relevant referenced agreements are the four to which the United States is party, i.e., the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on the Trade-Related Aspects of Intellectual Property Rights, the WIPO Copyright Treaty, and the WIPO Performances and Phonograms Treaty. Of these, the latter two entered into force after the Cybercrime Convention was opened for signature.

Because, among the referenced agreements, only TRIPS requires criminal sanctions, Article 10 permits a Party to reserve the right not to impose criminal liability in limited circumstances provided other "effective remedies" are available and the reservation does not derogate from its minimum obligations under applicable international instruments, which the Explanatory Report (paragraph 116) makes clear refers to TRIPS. Because U.S. law provides for other effective remedies but not criminal liability for infringements of certain rental rights, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 10 and 42, reserves the right to impose other effective remedies in lieu of criminal liability under paragraphs 1 and 2 of Article 10 ("Offenses related to infringement of copyright and related rights") with respect to infringements of certain rental rights to the extent the criminalization of such infringements is not required pursuant to the obligations the United States has undertaken under the agreements referenced in paragraphs 1 and 2.

Article 11 ("Attempt and aiding or abetting") provides that aiding or abetting the commission of any of the offenses set forth in Articles 2–10 shall also be made criminal. Similarly, a Party is required to criminalize an attempt to commit certain of these offenses, to the extent specified in paragraph 2 of the Article. As with the Article 2–10 offenses, aiding or abetting or an attempt must be committed intentionally. Thus, as indicated in the Explanatory Report (paragraph 119), the fact that an ISP is a mere conduit for criminal activity, such as the transmission of child pornography or a computer virus, does not give rise to criminal liability for the ISP, because it would not share the criminal intent required for aiding and abetting liability. Further, the Explanatory Report (paragraph 119) makes clear the Parties' understanding that "there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision."

Article 12 ("Corporate liability") requires the adoption of criminal, civil or administrative measures to ensure that a corporation or similar legal person can be held liable for the offenses to be es-

tablished in accordance with the Convention, where such offenses are committed for its benefit by a natural person who has a leading position in the corporation or legal person. The Article also provides for liability where a lack of supervision or control by a leading person makes possible the commission of one of the criminal offenses for the benefit of the legal person by a natural person acting under its authority. Per the Explanatory Report (paragraph 125), a "natural person acting under its authority" is understood to be an employee or agent acting within the scope of their authority. Further, the Explanatory Report (paragraph 125) notes that a "failure to supervise should be interpreted to include the failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the legal person." The Explanatory Report (paragraph 125) also makes clear, however, that such appropriate and reasonable measures "should not be interpreted as requiring a general surveillance regime over employee communications." The concepts set forth in Article 12 are already reflected in U.S. law.

Under Article 13 ("Sanctions and measures"), each Party is to ensure that Articles 2–11 offenses committed by natural persons are subject to "effective, proportionate and dissuasive sanctions, which include deprivation of liberty." As elucidated in the Explanatory Report (paragraph 130), the Article leaves open the possibility of other sanctions or measures, such as forfeiture, for these offenses. Consistent with the approach set forth in Article 12 ("Corporate liability"), sanctions to be imposed against legal persons may be criminal, civil or administrative in nature.

Procedural law (Articles 14–21):

As recognized by the Explanatory Report (paragraph 133), evidence in electronic form can be difficult to secure, as it may be flowing swiftly in the process of communication and can be quickly altered, moved or deleted. In an effort to ensure that Parties are able to investigate effectively the offenses established under the Convention and other criminal offenses committed by means of a computer system, as well as to collect evidence in electronic form of a criminal offense, the Convention requires each Party to ensure that its competent authorities have certain powers and procedures for use in specific criminal investigations or proceedings. These powers and procedures are set forth in articles on: "Expedited preservation of stored computer data" (Article 16), "Expedited preservation and partial disclosure of traffic data" (Article 17), "Production order" (Article 18), "Search and seizure of stored computer data" (Article 19), "Real-time collection of traffic data" (Article 20), and "Interception of content data" (Article 21). All of these powers and procedures are already provided for under U.S. law.

A number of important limitations on the powers and procedures to be established pursuant to Articles 16–21 are set forth throughout the procedural law articles. Under Article 14 ("Scope of procedural provisions"), for example, the powers and procedures are to be invoked to obtain or collect data in connection with "specific" criminal investigations or proceedings. Thus, as the Explanatory Report explains (paragraphs 151 and 152), the Convention does not impose a general obligation on service providers to collect and re-

tain data on a routine basis simply because such data might one day be useful to some yet-to-be determined criminal investigation or proceeding. The preservation measures apply to data already stored by means of a computer system, thus presupposing that the data already exists, has been collected and is being stored. Further, Article 15 ("Conditions and safeguards") provides that the establishment, implementation and application of the powers and procedures called for by the Convention are to be subject to conditions and safeguards provided for under a Party's domestic law, which law shall provide for the adequate protection of human rights and liberties, including rights arising in accordance with obligations a Party has undertaken under applicable human rights instruments. This Article depends on implementation through a Party's domestic law. For the United States, no implementing legislation would be required as the U.S. Constitution and U.S. law already provide for adequate conditions and safeguards.

Article 15 and its accompanying text in the Explanatory Report (paragraph 147) recognize that, depending on the power or procedure, different conditions and safeguards under domestic law may be appropriate. For example, the Explanatory Report (paragraph 215) notes that, due to its high degree of intrusiveness, interception of content data pursuant to Article 21 merits more stringent safeguards, such as judicial or other independent supervision, as well as limitations on its duration. Article 15 also requires a Party, to the extent consistent with the public interest, to consider the impact of the powers and procedures upon the rights, responsibilities and legitimate interests of third parties. In this regard, the Explanatory Report (paragraph 148) indicates that a Party should consider mitigating the impact of such powers and procedures through such steps as minimizing disruption of consumer services, protecting service providers from liability for disclosing or facilitating the disclosure of data, or protecting proprietary interests.

The preservation regime to be established pursuant to Article 16 ("Expedited preservation of stored computer data") and Article 17 ("Expedited preservation and partial disclosure of traffic data") requires a Party to enable its competent authorities to order or similarly obtain the expedited preservation of specified computer data, including traffic data, for use in a specific investigation or proceeding. This power, which already exists in U.S. law, is important to ensuring that evidence is not moved, altered or deleted while further processes for obtaining a search warrant or subpoena for its disclosure are pursued.

As indicated in the Explanatory Report (paragraph 160), preservation under Article 16 may be accomplished by different legal means, including by ordering a person, including a service provider, not to destroy or delete computer data within that person's possession or control. The person may be required to preserve that data for a period of up to 90 days to allow the competent authorities to seek its disclosure. (A Party may provide for renewal of the preservation order.) The person who is to preserve the data may also be required to keep confidential for a period of time the undertaking of the preservation. With respect to traffic data, Article 17 provides that a sufficient amount of data must be able to be disclosed expeditiously in order to enable a Party to identify other service pro-

viders and the path through which a communication was transmitted. Such expedited disclosure is intended to enable authorities to take steps to preserve additional computer data that otherwise might be lost, which can be critical to tracing a communication back to the source of a computer-related crime (Explanatory Report, paragraphs 166–168). The U.S. Government would comply with this requirement by moving expeditiously, using existing preservation and disclosure procedures provided for under U.S. law.

As stated in the Explanatory Report (paragraphs 151 and 152), the data preservation measures contained in Articles 16 and 17 are distinguishable from so-called "data retention" measures in that they "do not mandate the collection of all, or even some, data collected by a service provider or other entity in the course of its activities." Instead, as indicated above, data preservation measures apply only to data that already exists, is being stored, and is specified by competent authorities as being sought in connection with a specific criminal investigation or proceeding.

Article 18 ("Production order") and Article 19 ("Search and seizure of stored computer data") require Parties to establish additional measures by which their competent authorities can obtain stored computer data. Under Article 18, authorities must be able to order a person, including third party custodian of data, such as an ISP, to produce data, including subscriber information, that is in that person's possession or control. The Explanatory Report (paragraph 177) makes clear that such subscriber information, which includes various types of information about the use and user of a service, may be in computer data form as well as in other forms (e.g., paper records). The Article, however, does not impose an obligation on service providers to compile and maintain such subscriber information in the normal course of their business. Instead, as the Explanatory Report (paragraph 181) describes, it requires a Party to be able to order a service provider to produce subscriber information that it does in fact keep. For its part, Article 19 is intended to enable authorities themselves to search and seize a computer system, data stored in a computer system and data contained in storage mediums, such as diskettes (Explanatory Report, paragraphs 187–189).

Article 20 ("Real time collection of traffic data") and Article 21 ("Interception of content data") require Parties to establish measures to enable their competent authorities to collect data associated with specified communications in their territory at the time of the data's communication (i.e., in "real time"). "Traffic data" is defined in Article 1, while guidance in the Explanatory Report (paragraph 209) indicates that "content data" refers to "the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)." Under Article 20, a Party is required to enable its authorities to collect traffic data with respect to any offense, although under Article 14(3)(a), a Party may take a reservation limiting the types of crimes to which Article 20 must be applied. This reservation would not be needed by the United States as federal law already makes this mechanism generally available for criminal investigations and prosecutions. With regard to Article 21, the Explanatory Report (paragraphs 210 and 212) recognizes that interception of content

data is considered an intrusive measure and, therefore, that Article only requires a Party to provide for such measures in relation to a range of serious offenses to be determined by its domestic law, which is the approach taken by U.S. federal law.

Under both Articles 20 and 21, a Party is generally required to adopt measures enabling its competent authorities: (a) to collect or record data themselves through application of technical means on the territory of that Party, and (b) to compel a service provider, within its existing technical capability, either to collect or record data through the application of technical means or to cooperate and assist competent authorities in the collection or recording of such data. The Explanatory Report (paragraph 224) explains that in certain states, such as Germany, due to "established legal principles", law enforcement is not able to intercept communications directly and must rely on service providers to have the capability to collect content or traffic data in real time on its behalf. Accordingly, pursuant to Article 20(2), Parties may therefore adopt other measures to ensure the collection or recording of data, including by requiring service providers to provide technical facilities. This exception does not apply to the United States as its authorities are empowered to collect and record data directly through technical means. In states, such as the United States, in which this exception would not be invoked, the obligation on a service provider to assist law enforcement under Articles 20 and 21 is subject to "its existing technical capability." As more fully described in the Explanatory Report (paragraph 221), this means there is no obligation to impose a duty on service providers to obtain or deploy new equipment or engage in costly reconfiguration of their systems in order to assist law enforcement.

Jurisdiction (Article 22):

Article 22 requires a Party to establish jurisdiction over the offenses specified in the Convention where committed in the Party's territory, on board a ship flying its flag, on board an aircraft registered under its laws, or, in certain circumstances, by one of its nationals. Except with respect to offenses committed in its territory, Article 22(2) permits a Party to enter a reservation as to these jurisdictional bases. Because U.S. criminal law does not provide for plenary criminal jurisdiction over offenses involving its nationals and selectively provides for maritime or aircraft jurisdiction, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 22 and 42, reserves the right not to apply in part paragraphs (1)(b), (c) and (d) of Article 22 ("Jurisdiction"). The United States does not provide for plenary jurisdiction over offenses that are committed outside its territory by its citizens or on board ships flying its flag or aircraft registered under its laws. However, United States law does provide for jurisdiction over a number of offenses to be established under the Convention that are committed abroad by United States nationals in circumstances implicating particular federal interests, as well as over a number of such offenses committed on board United States-flagged ships or aircraft registered under United States

law. Accordingly, the United States shall implement paragraphs 1(b), (c) and (d) to the extent provided for under its federal law.

Under Article 22(3), a Party is also required to establish jurisdiction over the criminal offenses established in accordance with Articles 2–11 of the Convention in the event it does not extradite an alleged offender solely on the basis of nationality. As explained in the Explanatory Report (paragraph 237), establishing such jurisdiction is necessary to ensure that such a Party has the ability to undertake investigations and proceedings against the alleged offender domestically. United States law permits extradition of nationals; accordingly, this paragraph does not give rise to a need for implementing legislation.

As indicated in the Explanatory Report (paragraph 239), offenses committed through the use of the Internet may target victims in many states, giving rise to instances in which more than one Party has jurisdiction. Accordingly, Article 22(5) provides that when more than one Party claims jurisdiction over an alleged offense established in accordance with the Convention, they shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

CHAPTER III—INTERNATIONAL CO-OPERATION (ARTICLES 23–35)

Chapter III, Article 23 ("General principles relating to international co-operation") provides that Parties are to provide international cooperation to one another to the "widest extent possible" for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. The Chapter contains extradition and mutual legal assistance provisions typical of many multilateral law enforcement conventions to which the United States is already a party, and, as such, is compatible with existing U.S. law. As provided in the Chapter and as recognized in the Explanatory Report (paragraph 244), the general approach is to supplement existing international cooperation agreements and provide a basis for such cooperation where no such framework exists.

Extradition is covered in Article 24 ("Extradition"), which provides that the offenses established in accordance with Articles 2–11 of the Convention shall be deemed to be included as extraditable offenses in extradition treaties between or among the Parties provided the offenses are subject to minimum penalties as described in the Article. The Article provides that extradition is subject to the conditions provided by the law or applicable treaties of the requested Party, including the grounds on which it may refuse extradition. Any Party that refuses an extradition request solely because the person sought is one of its nationals is obliged at the request of the requesting Party to submit the case to its competent authorities for the purpose of prosecution.

Article 24 also provides that a Party that conditions extradition on the existence of a treaty may use the Convention itself as a treaty basis, although it is not obligated to do so. For situations in which there is no separate extradition treaty in existence, Article 24(7) provides that a Party is to notify the COE of the name and address of its authority for receiving requests for extradition or

provisional arrest under the Convention. The United States would not invoke Article 24 as a separate basis for extradition, but, instead, would continue to conduct extradition pursuant to applicable bilateral treaties, supplemented where appropriate by relevant international law enforcement conventions. Thus, the principal legal effect of Article 24 for the United States would be to incorporate by reference the offenses provided for in the Convention as extraditable offenses under U.S. bilateral extradition treaties. Further, because the United States would continue to rely on bilateral extradition treaties, it would notify the COE that it is not designating an authority under Article 24(7) and that the authority responsible for making or receiving extradition requests on behalf of the United States is set forth in the applicable bilateral extradition treaties.

The provisions relating to mutual legal assistance are set forth in Articles 25–35. Article 25 sets forth "General principles relating to mutual assistance," where the duty to provide cooperation is not limited to the offenses to be established pursuant to Articles 2–11 of the Convention. As the Explanatory Report (paragraph 253) notes, the need for "streamlined mechanisms of international co-operation" extends beyond such offenses and, thus, Article 25 obliges the Parties to afford mutual assistance "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 evidence in electronic form of a criminal offence." Article 25 provides that in urgent circumstances a Party may make a request for assistance by expedited means of communication (e.g., fax or e-mail) and that the requested Party shall be obliged to respond to the request by expedited means of communication as well. Article 25(4) sets forth the general rule that, except as otherwise specifically provided for in Chapter III, mutual assistance shall be subject to conditions provided for by applicable mutual legal assistance treaties or by the law of the requested Party. Article 25(4) itself provides for an exception to this general rule in that it precludes a Party from denying assistance with respect to the offenses set forth in Articles 2–11 on the ground that the request concerns a fiscal (i.e., tax) offense.

Article 26 ("Spontaneous information") provides that, without receiving an assistance request, a Party may forward to another Party information it obtains in one of its own investigations where it believes such information might assist the other Party in initiating or carrying out an investigation or proceeding. Per the Explanatory Report (paragraph 260), such a provision was thought useful because some states require a positive grant of legal authority to provide such assistance, which would be satisfied by inclusion of this provision in the Convention. Before providing such information, a Party may require that it be used subject to conditions, such as that it be kept confidential.

Article 27 ("Procedures pertaining to mutual assistance requests in the absence of applicable international agreements") and Article 28 ("Confidentiality and limitations on use") provide a framework for assistance where there is no mutual legal assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting Party and the requested Party. Arti-

cle 27 provides procedures for handling assistance requests as well as grounds for refusal, which include where the request concerns a political offence or is "likely to prejudice [a requested Party's] sovereignty, security, ordre public or other essential interests." The Article also provides for the designation by each Party of a central authority or authorities, which is to be responsible for handling requests for mutual assistance. In the event of urgency, Article 27(9) allows for requests to be sent directly to judicial authorities. A Party may declare, however, that for reasons of efficiency, such requests are to be addressed to its designated central authority. In this regard, I recommend that the following declaration be included in the U.S. instrument of ratification:

> The Government of the United States of America declares, pursuant to Articles 27 and 40, that requests made to the United States of America under paragraph 9(e) of Article 27 ("Procedures pertaining to mutual assistance requests in the absence of applicable international agreements") are to be addressed to its central authority for mutual assistance.

Article 28 provides that the requested Party may condition the provision of information on confidentiality and certain use limitations. The Article only applies, however, where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force as between the requested and requesting Parties, unless the Parties concerned agree to its application in whole or in part.

Articles 29–35 contain specific provisions on mutual assistance that apply regardless of whether assistance is being requested or provided pursuant to an existing mutual legal assistance treaty or arrangement.

Article 29 ("Expedited preservation of stored computer data") and Article 30 ("Expedited disclosure of preserved traffic data") address the preservation and disclosure of data. As indicated in the Explanatory Report (paragraphs 282 and 290), these articles make available for the purposes of international cooperation the mechanisms provided for use at the domestic level in Articles 16 and 17. Under Article 29, a requesting Party may obtain advance, expedited preservation of stored data that is located in the territory of the requested Party provided it intends to submit a subsequent, formal mutual assistance request for disclosure of the data. Upon preservation, the requesting Party shall then have at least sixty days to submit its mutual assistance request. A requested Party may refuse preservation on the ground that the request concerns a political offense or that its execution would be "likely to prejudice its sovereignty, security, ordre public, or other essential interests." For the purposes of obtaining the initial preservation, Article 29 does not as a rule require dual criminality. As explained in the Explanatory Report (paragraph 285), once preserved, the data is generally not subject to disclosure to government officials until the formal mutual assistance request is executed. A determination with respect to any dual criminality requirement can be made in the context of that request. However, a requested Party that requires dual criminality as a condition under its applicable mutual legal assistance framework may enter a reservation that would enable it to refuse a preservation request if it has reason to believe that at the

time of the disclosure dual criminality would not be met. Because the United States generally seeks, as a policy matter, to minimize the application of dual criminality as a ground for refusing international mutual assistance, and, especially since preservation in and of itself does not result in disclosure of data to government officials, the United States would not exercise this reservation. Under Article 30, if the requested Party determines in executing an Article 29 request for expedited preservation concerning a specific communication that a service provider in another state was involved in that communication, then it is under an obligation to disclose to the requesting Party such traffic data as necessary to identify the foreign service provider and the communication path. As in Article 29, such disclosure may only be withheld by the requested Party on political offense grounds or on the grounds that it "is likely to prejudice its sovereignty, security, ordre public or other essential interests."

Article 31 ("Mutual assistance regarding accessing of stored computer data") is the international cooperation counterpart to Article 19 ("Search and seizure of stored computer data") in the procedural law chapter. It requires a requested Party to be able to "search or similarly access, seize or similarly secure, and disclose" stored data in response to a request for mutual assistance. Where the data is "particularly vulnerable to loss or modification," the requested Party is required to expedite its response.

Article 32 ("Trans-border access to stored computer data with consent or where publicly available") is not a mutual assistance provision per se. Rather, as discussed in the Explanatory Report (paragraphs 293 and 294), it reflects the general agreement that an accessing Party need not seek the prior authorization of another Party to access data stored in that other Party's territory where the data is publicly available or obtained through a computer system located in the accessing Party's territory with the lawful and voluntary consent of a person who has lawful authority to disclose that data through that system.

Article 33 ("Mutual assistance in the real-time collection of traffic data") and Article 34 ("Mutual assistance regarding the interception of content data") are the counterparts in the international cooperation chapter to Articles 20 and 21. Under Article 33, a Party is required to provide mutual assistance in the real-time collection of traffic data at least with respect to offences for which such real-time collection would be permitted under its domestic law. Similarly, Article 34 obligates a Party to provide mutual assistance in the interception of content data, but only to the extent permitted under its applicable treaties and domestic law.

Article 35 ("24/7 Network") requires each Party to designate a point of contact that will be available 24 hours a day, seven days a week to ensure the provision of immediate assistance for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form. This shall include an obligation to facilitate or, if permitted by its domestic law and practice, direct the carrying out of immediate assistance in the provision of technical advice, the expedited preservation of stored computer data, the expedited disclosure of preserved traffic data, the collection of evi-

dence, the provision of legal information, and the locating of suspects. As indicated in the Explanatory Report (paragraph 298), this channel draws its inspiration from a network created by the G8 countries in 1998. The 24/7 point of contact for the United States would be the same point of contact used for the G8 network: the Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section.

Chapter IV—Final provisions (Articles 36–48):

As indicated in the Explanatory Report (paragraph 303), the provisions contained in Chapter IV ("Final provisions") are generally based on standard model clauses used by the COE. Article 36 ("Signature and entry into force") provides that the Convention is open for signature by COE member states and by non-member states that have participated in its elaboration, i.e., the United States, Canada, Japan, and South Africa. Five states, including at least three COE member states, must express their consent to be bound by the Convention for it to enter into force. After entry into force, states subsequently expressing their consent to be bound shall become party to it on the first day of the month following a three month period from the date of that state's expression of consent. Article 37 ("Accession to the Convention") details a procedure for accession by other states after the Convention enters into force. Reflecting past practice in this area within the COE, accession by a state requires the unanimous consent of the Parties to the Convention. Article 38 ("Territorial application") enables states to specify the extent of their territory to which the Convention will apply.

Article 39 ("Effects of the Convention") addresses the relationship of the Cybercrime Convention to other international instruments. It makes clear that the Convention is intended to supplement applicable treaties or arrangements between the Parties in the area of international cooperation. As set forth in the Article and as explained in the Explanatory Report (paragraph 312), Parties are free to enter into new agreements with one another regarding matters dealt with in the Convention provided they do not undermine its objectives and principles. Article 39 also contains a "savings" clause to the effect that the Convention does not affect other rights and obligations that are not addressed in the Convention.

Article 40 ("Declarations"), Article 41 ("Federal clause") and Article 42 ("Reservations") permit Parties to modify or derogate from specified Convention obligations. Under Article 40, a Party may declare that it avails itself of various additional elements provided for in specified articles at the time it consents to be bound by the Convention. As set forth above, in order to meet its Convention obligations without having to seek new implementing legislation, the United States would make declarations under Articles 2, 6(1)(b), 7, and 27(9)(e).

Article 41 ("Federal clause") permits a federal state to enter a reservation allowing for minor variations in coverage of its Chapter II obligations ("Measures to be taken at the national level"). As stated in the Explanatory Report (paragraph 316), this reservation takes into account that variations in coverage may occur due to "well-established domestic law and practice" of a federal state based on the federal state's "Constitution or other fundamental

principles concerning the division of powers in criminal justice matters" between its central government and its constituent entities. The reservation was inserted to make clear that the United States could meet its Convention obligations through application of existing federal law and would not be obligated to criminalize activity that does not implicate a foreign, interstate or other federal interest meriting the exercise of federal jurisdiction. In the absence of the reservation, there would be a narrow category of conduct regulated by U.S. State, but not federal, law that the United States would be obligated to criminalize under the Convention (e.g., an attack on a stand-alone personal computer that does not take place through the Internet). Article 41 makes clear that this reservation is available only where the federal state is still able to meet its international cooperation obligations and where application of the reservation would not be so broad as to exclude entirely or substantially diminish its obligations to criminalize conduct and provide for procedural measures. Such a restriction is not an obstacle for the United States because the Convention's international cooperation provisions are implemented at the federal level and because federal substantive criminal law provides for broad overall coverage of the illegal conduct addressed by the Convention. In invoking the reservation, the U.S. Government would be obliged to bring the Convention's provisions to the attention of its constituent States and entities, with a "favourable opinion" encouraging them to take appropriate action to give effect to such provisions, even though, as a result of the reservation, there would be no obligation for them to do so. This step would be accomplished through an outreach effort on the part of the federal government. Accordingly, I recommend that the following reservation be included in the U.S. instrument of ratification:

> The Government of the United States of America, pursuant to Articles 41 and 42, reserves the right to assume obligations under Chapter II of the Convention in a manner consistent with its fundamental principles of federalism. Furthermore, in connection with this reservation, I recommend that the Senate include the following understanding in its resolution of advice and consent:

The United States understands that, in view of its reservation pursuant to Article 41, Chapter II of the Convention does not warrant the enactment of any legislative or other measures; instead, the United States will rely on existing federal law to meet its obligations under Chapter II of the Convention.

Article 42 ("Reservations") enumerates those provisions by which a Party can exclude or modify its obligations with respect to specified articles at the time it consents to be bound by the Convention. Consistent with COE treaty practice, the Article provides that no other reservations may be made. Article 43 ("Status and withdrawal of reservations") provides a mechanism for Parties to withdraw their reservations as soon as circumstances permit. As set forth above, to meet its obligations without the need for additional implementing legislation, the United States would make permitted reservations under Articles 4(2), 6(3), 9(4), 10(3), 22(2), and 41.

The procedure for amending the Convention is set forth in Article 44 ("Amendments") and provides that amendments do not come

into force until they have been accepted by all Parties to the Convention. Article 45 ("Settlement of disputes") obligates Parties to seek to settle disputes as to the interpretation or application of the Convention through peaceful means of their choosing. Resort to binding arbitration or to the International Court of Justice is possible if the Parties concerned agree. Article 46 ("Consultations of the Parties") establishes a flexible framework for Parties to consult regarding implementation of the Convention, including the effect on implementation of significant legal, policy or technological developments. As appropriate, such consultations are to be facilitated by the COE, including specifically by the European Committee on Crime Problems. The Explanatory Report (paragraph 328) encourages Parties, in the context of these consultations, to seek the views of non-governmental and private sector organizations on privacy, business and other related issues.

Article 47 ("Denunciation") sets out the procedure for a Party to denounce the Convention with three months advance notice, and Article 48 ("Notification") empowers the COE's Secretary General to act as the notifying authority in relation to the Convention.

It is my belief that the Convention would be advantageous to the United States and, subject to the reservations and declarations proposed in this Report, would be consistent with existing United States legislation. The Departments of Justice and Commerce join me in recommending that the Convention be transmitted to the Senate at an early date for its advice and consent to ratification, subject to the reservations and declarations described above.

Respectfully submitted.

COLIN L. POWELL.

CONVENTION ON CYBERCRIME

CONVENTION SUR LA CYBERCRIMINALITÉ

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 parties 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 cybercrime, *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 by 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;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

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

Convinced that the present Convention is necessary to deter action 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 their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which 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 rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and 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 evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions 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 cybercrime;

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 and 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 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

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 a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

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 intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

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-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

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, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

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 – Misuse of devices

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 and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii 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 any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

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 authentic, regardless whether or not the data is directly readable and intelligible. A Party may require 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 of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

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 intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in 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.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

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 revising the Bern 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 wilfully, on a commercial scale 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 (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

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 through 10 of the present Convention with intent that such offence be committed.

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, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, 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 a criminal offence 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 it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary 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 a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 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 or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is 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 computer 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 computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of 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 to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "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 services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt 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; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt 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, pursuant to 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, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt 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. 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 adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

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

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 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 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 Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its 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.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – 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 the 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 evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 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.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall 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 for any other offence of a comparable nature under the law of that Party.

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 address of each authority responsible for making or receiving requests 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.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating 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 evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the

extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, 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 co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

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 denominate 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 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and 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 co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only 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.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – 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 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, 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 responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission 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 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.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b 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 criminal investigations or proceedings conducted 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. Reasons shall be given for any refusal or postponement of the request. 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 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. 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.

9 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 sub-paragraph a. of this article 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.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – 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, 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 seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f 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 stored computer 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 required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 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.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty 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 a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another 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 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:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – 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 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is 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 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without 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.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this 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 criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations

or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision 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 co-ordinate 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 IV – Final provisions

Article 36 – 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.

2 This Convention is subject to ratification, acceptance or approval. 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 five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

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 its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. 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 any State acceding to the Convention 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 38 – 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 State 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 the declaration 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 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, 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 possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, 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(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – 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, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

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 with the non-member States 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 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) 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 CDPC, 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 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – 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 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede 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 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

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 Budapest, this 23rd day of November 2001, 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.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

Certified a true copy of the sole original document, in English and in French, deposited in the archives of the Council of Europe.

Copie certifiée conforme à l'exemplaire original unique en langues française et anglaise, déposé dans les archives du Conseil de l'Europe.

Strasbourg, 16 janvier 2002

The Director General of Legal Affairs
of the Council of Europe,

Le Directeur Général des Affaires Juridiques
du Conseil de l'Europe,

Guy DE VEL

Convention on Cybercrime (ETS no. 185)

Français

Explanatory Report
(adopted on 8 November 2001)

I. The Convention and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001) and the Convention has been opened for signature in Budapest, on 23 November 2001, on the issue of the International Conference on Cybercrime.

II. The text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions contained therein.

I. Introduction

1. 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.

2. 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. Circuit-switched connections have been replaced by packet-switched networks. 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.

3. 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.

4. The ease of accessibility and searchability 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.

5. These developments have given rise to an 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.

6. 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.

II. The preparatory work

7. 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:

8. "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.

9. 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 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."

10. 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." (1) A similar conclusion

emerged already from the Report attached to Recommendation N° R (89) 9 (2) concerning substantive law and from Recommendation N° R (95) 13 (3) concerning problems of procedural law connected with information technology.

11. The new committee's specific terms of reference were as follows:

> i. "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:
>
> ii. 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;
>
> iii. 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;
>
> iv. 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;
>
> v. 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 of *ne bis idem* in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;
>
> vi. 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).
>
> The Committee should draft a binding legal instrument, as far as possible, on the items i) - v), with particular emphasis on international questions and, if appropriate, accessory recommendations regarding specific issues. The Committee may make suggestions on other issues in the light of technological developments."

12. 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.

13. 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.

14. 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.

15. 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.

III. The Convention

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. Finally, Chapter IV contains the final clauses, which - with certain exceptions - repeat the standard provisions in Council of Europe treaties.

COMMENTARY ON THE ARTICLES OF THE CONVENTION

Chapter I – Use of terms

Introduction to the definitions at Article 1

22. It was understood by the drafters that under this Convention Parties would not be obliged to copy *verbatim* into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation.

Article 1 (a) - Computer system

23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.

24. A network is an interconnection between two or more computer systems. The connections

may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.

Article 1 (b) - Computer data

25. The definition of computer data builds upon the ISO-definition of data. This definition contains the terms "suitable for processing". This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion " computer data" is introduced. Computer data that is automatically processed may be the target of one of the criminal offences defined in this Convention as well as the object of the application of one of the investigative measures defined by this Convention.

Article 1 (c) - Service provider

26. The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems (cf. also comments on Section 2). Under (i) of the definition, it is made clear that both public and private entities which provide users the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether free of charge or for a fee. The closed group can be e.g. the employees of a private enterprise to whom the service is offered by a corporate network.

27. Under (ii) of the definition, it is made clear that the term "service provider" also extends to those entities that store or otherwise process data on behalf of the persons mentioned under (i). Further, the term includes those entities that store or otherwise process data on behalf of the users of the services of those mentioned under (i). For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his web site) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services.

Article 1 (d) - Traffic data

28. For the purposes of this Convention traffic data as defined in article 1, under subparagraph d., is a category of computer data that is subject to a specific legal regime. This data is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself.

29. In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further

evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive.

30. The definition lists exhaustively the categories of traffic data that are treated by a specific regime in this Convention: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. Not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

31. The definition leaves to national legislatures the ability to introduce differentiation in the legal protection of traffic data in accordance with its sensitivity. In this context, Article 15 obliges the Parties to provide for conditions and safeguards that are adequate for protection of human rights and liberties. This implies, *inter alia*, that the substantive criteria and the procedure to apply an investigative power may vary according to the sensitivity of the data.

Chapter II – Measures to be taken at the national level

32. Chapter II (Articles 2 – 22) contains three sections: substantive criminal law (Articles 2 – 13), procedural law (Articles 14 – 21) and jurisdiction (Article 22).

Section 1 – Substantive criminal law

33. The purpose of Section 1 of the Convention (Articles 2 – 13) is to improve the means to prevent and suppress computer- or computer – related crime by establishing a common minimum standard of relevant offences. This kind of harmonisation alleviates the fight against such crimes on the national and on the international level as well. Correspondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too. International co-operation (esp. extradition and mutual legal assistance) is facilitated e.g. regarding requirements of double criminality.

34. The list of offences included represents a minimum consensus not excluding extensions in domestic law. To a great extent it is based on the guidelines developed in connection with Recommendation No. R (89) 9 of the Council of Europe on computer-related crime and on the work of other public and private international organisations (OECD, UN, AIDP), but taking into account more modern experiences with abuses of expanding telecommunication networks.

35. The section is divided into five titles. Title 1 includes the core of computer-related offences, offences against the confidentiality, integrity and availability of computer data and systems, representing the basic threats, as identified in the discussions on computer and data security to which electronic data processing and communicating systems are exposed. The heading describes the type of crimes which are covered, that is the unauthorised access to and illicit tampering with systems, programmes or data. Titles 2 – 4 include other types of 'computer-related offences',

which play a greater role in practice and where computer and telecommunication systems are used as a means to attack certain legal interests which mostly are protected already by criminal law against attacks using traditional means. The Title 2 offences (computer-related fraud and forgery) have been added by following suggestions in the guidelines of the Council of Europe Recommendation No. R (89) 9. Title 3 covers the 'content-related offences of unlawful production or distribution of child pornography by use of computer systems as one of the most dangerous *modi operandi* in recent times. The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the present Convention.

Title 4 sets out 'offences related to infringements of copyright and related rights'. This was included in the Convention because copyright infringements are one of the most widespread forms of computer- or computer-related crime and its escalation is causing international concern. Finally, Title 5 includes additional provisions on attempt, aiding and abetting and sanctions and measures, and, in compliance with recent international instruments, on corporate liability.

36. Although the substantive law provisions relate to offences using information technology, the Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.

37. The drafters of the Convention understood that Parties may exclude petty or insignificant misconduct from implementation of the offences defined in Articles 2-10.

38. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic 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 domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

39. All the offences contained in the Convention must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. For instance, in Article 8 on computer-related fraud, the intent to procure an economic benefit is a constituent element of the offence. The drafters of the Convention agreed that the exact meaning of 'intentionally' should be left to national interpretation.

40. Certain articles in the section allow the addition of qualifying circumstances when implementing the Convention in domestic law. In other instances even the possibility of a reservation is granted (cf. Articles 40 and 42). These different ways of a more restrictive approach in criminalisation reflect different assessments of the dangerousness of the behaviour involved or of the need to use criminal law as a countermeasure. This approach provides flexibility to governments and parliaments in determining their criminal policy in this area.

41. Laws establishing these offences should be drafted with as much clarity and specificity as possible, in order to provide adequate foreseeability of the type of conduct that will result in a criminal sanction.

42. In the course of the drafting process, the drafters considered the advisability of criminalising conduct other than those defined at Articles 2 – 11, including the so-called cyber-squatting, i.e. the fact of registering a domain-name which is identical either to the name of an entity that already exists and is usually well-known or to the trade-name or trademark of a product or company. Cyber-squatters have no intent to make an active use of the domain-name and seek to obtain a financial advantage by forcing the entity concerned, even though indirectly, to pay for the transfer of the ownership over the domain-name. At present this conduct is considered as a trademark-related issue. As trademark violations are not governed by this Convention, the drafters did not consider it appropriate to deal with the issue of criminalisation of such conduct.

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

43. The criminal offences defined under (Articles 2-6) are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.

Illegal access (Article 2)

44. "Illegal access" covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

45. The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above.

46. "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data).

However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

47. The act must also be committed 'without right'. In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."

48. The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of 'cookies' or 'bots' to locate and retrieve information on behalf of communication. The application of such tools *per se* is not 'without right'. The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself 'without right', in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of 'cookies' by not rejecting the initial instalment or not removing it.

49. Many national legislations already contain provisions on "hacking" offences, but the scope and constituent elements vary considerably. The broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the OECD Working Party in 1985.

50. Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extranets).

Illegal interception (Article 3)

51. This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights. The offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.

52. The text of the provision has been mainly taken from the offence of 'unauthorised

interception' contained in Recommendation (89) 9. In the present Convention it has been made clear that the communications involved concern "transmissions of computer data" as well as electromagnetic radiation, under the circumstances as explained below.

53. Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.

54. The offence applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. Therefore, the term 'non-public' does not *per se* exclude communications via public networks. Communications of employees, whether or not for business purposes, which constitute "non-public transmissions of computer data" are also protected against interception without right under Article 3 (see e.g. ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92).

55. The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard). Nonetheless, Parties may require as an additional element that the communication be transmitted between computer systems remotely connected.

56. It should be noted that the fact that the notion of 'computer system' may also encompass radio connections does not mean that a Party is under an obligation to criminalise the interception of any radio transmission which, even though 'non-public', takes place in a relatively open and easily accessible manner and therefore can be intercepted, for example by radio amateurs.

57. The creation of an offence in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision.

58. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities. It was also understood that the use of common commercial practices, such as employing 'cookies', is not intended to be criminalised as such, as not being an interception "without right". With respect to non-public communications of employees protected under Article 3 (see above paragraph 54), domestic law may provide a ground for legitimate interception of such communications. Under Article 3, interception in such circumstances would

be considered as undertaken "with right".

59. 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, or that the offence be committed in relation to a computer system that is connected to another computer system in accordance with Article 2, may also require similar qualifying elements to attach criminal liability in this article. These elements should be interpreted and applied in conjunction with the other elements of the offence, such as "intentionally" and "without right".

Data interference (Article 4)

60. The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

61. In paragraph 1, 'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.

62. The above acts are only punishable if committed "without right". Common activities inherent in the design of networks or common operating or commercial practices, such as, for example, for the testing or protection of the security of a computer system authorised by the owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system acquires new software (e.g., software permitting access to the Internet that disables similar, previously installed programs), are with right and therefore are not criminalised by this article. The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right. However, Parties may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime.

63. In addition, the offender must have acted "intentionally".

64. Paragraph 2 allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation, but Parties should notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

System interference (Article 5)

65. This is referred to in Recommendation No. (89) 9 as computer sabotage. The provision aims at

criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The text is formulated in a neutral way so that all kinds of functions can be protected by it.

66. The term "hindering" refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data.

67. The hindering must furthermore be "serious" in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).

68. The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalised by this article, even if it causes serious hindering.

69. The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law.

70. The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

Misuse of devices (Article 6)

71. This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data. As the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should

prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access - ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries. A similar approach has already been taken in the 1929 Geneva Convention on currency counterfeiting.

72. Paragraph 1(a)1 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2-5 of the present Convention. 'Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a 'computer program' refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

73. The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

74. Paragraph 1(a)2 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed.

75. Paragraph 1(b) creates the offence of possessing the items set out in paragraph 1(a)1 or 1(a)2. Parties are permitted, by the last phrase of paragraph 1(b), to require by law that a number of such items be possessed. The number of items possessed goes directly to proving criminal intent. It is up to each Party to decide the number of items required before criminal liability attaches.

76. The offence requires that it be committed intentionally and without right. In order to avoid the danger of overcriminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific (i.e. direct) intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention.

77. Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with

right'.

78. Due to different assessments of the need to apply the offence of "Misuse of Devices" to all of the different kinds of computer offences in Articles 2 – 5, paragraph 3 allows, on the basis of a reservation (cf. Article 42), to restrict the offence in domestic law. Each Party is, however, obliged to criminalise at least the sale, distribution or making available of a computer password or access data as described in paragraph 1 (a) 2.

Title 2 - Computer-related offences

79. Articles 7 - 10 relate to ordinary crimes that are frequently committed through the use of a computer system. Most States already have criminalised these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones.

80. "Computer-related forgery" and "Computer-related fraud" deal with certain computer-related offences, i.e. computer-related forgery and computer-related fraud as two specific kinds of manipulation of computer systems or computer data. Their inclusion acknowledges the fact that in many countries certain traditional legal interests are not sufficiently protected against new forms of interference and attacks.

Computer-related forgery (Article 7)

81. The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations.

82. It should be noted that national concepts of forgery vary greatly. One concept is based on the authenticity as to the author of the document, and others are based on the truthfulness of the statement contained in the document. However, it was agreed that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term "authentic" the genuineness of the data.

83. This provision covers data which is the equivalent of a public or private document, which has legal effects. The unauthorised "input" of correct or incorrect data brings about a situation that corresponds to the making of a false document. Subsequent alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond in general to the falsification of a genuine document.

84. The term "for legal purposes" refers also to legal transactions and documents which are legally relevant.

85. The final sentence of the provision allows Parties, when implementing the offence in domestic law, to require in addition an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Computer-related fraud (Article 8)

86. With the arrival of the technological revolution the opportunities for committing economic crimes such as fraud, including credit card fraud, have multiplied. Assets represented or administered in computer systems (electronic funds, deposit money) have become the target of manipulations like traditional forms of property. These crimes consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property.

87. To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer programme or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles. Article 8(b) covers acts such as hardware manipulations, acts suppressing printouts and acts affecting recording or flow of data, or the sequence in which programs are run.

88. The computer fraud manipulations are criminalised if they produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person. The term 'loss of property', being a broad notion, includes loss of money, tangibles and intangibles with an economic value.

89. The offence must be committed "without right", and the economic benefit must be obtained without right. Of course, legitimate common commercial practices, which are intended to procure an economic benefit, are not meant to be included in the offence established by this article because they are conducted with right. For example, activities carried out pursuant to a valid contract between the affected persons are with right (e.g. disabling a web site as entitled pursuant to the terms of the contract).

90. The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit to another, but are not carried out with fraudulent or dishonest intent, are not meant to be included in the offence established by this article. For example, the use of information gathering programs to comparison shop on the Internet ("bots"), even if not authorised by a site visited by the "bot" is not intended to be criminalised.

Title 3 – Content-related offences

Offences related to child pornography (Article 9)

91. Article 9 on child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children.

92. This provision responds to the preoccupation of Heads of State and Government of the Council of Europe, expressed at their 2nd summit (Strasbourg, 10 - 11 October 1997) in their Action Plan (item III.4) and corresponds to an international trend that seeks to ban child pornography, as evidenced by the recent adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography (COM2000/854).

93. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most States already criminalise the traditional production and physical distribution of child pornography, but with the ever-increasing use of the Internet as the primary instrument for trading such material, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children. It is widely believed that such material and on-line practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children.

94. Paragraph 1(a) criminalises the production of child pornography for the purpose of distribution through a computer system. This provision was felt necessary to combat the dangers described above at their source.

95. Paragraph 1(b) criminalises the 'offering' of child pornography through a computer system. 'Offering' is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it. 'Making available' is intended to cover the placing of child pornography on line for the use of others e.g. by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography.

96. Paragraph 1(c) criminalises the distribution or transmission of child pornography through a computer system. 'Distribution' is the active dissemination of the material. Sending child pornography through a computer system to another person would be addressed by the offence of 'transmitting' child pornography.

97. The term 'procuring for oneself or for another' in paragraph 1(d) means actively obtaining child pornography, e.g. by downloading it.

98. The possession of child pornography in a computer system or on a data carrier, such as a diskette or CD-Rom, is criminalised in paragraph 1(e). The possession of child pornography stimulates demand for such material. An effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession.

99. The term 'pornographic material' in paragraph 2 is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt. Therefore, material having an artistic, medical, scientific or similar merit may be considered not to

be pornographic. The visual depiction includes data stored on computer diskette or on other electronic means of storage, which are capable of conversion into a visual image.

100. A 'sexually explicit conduct' covers at least real 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 in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated.

101. The three types of material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer.

102. In the three cases covered by paragraph 2, the protected legal interests are slightly different. Paragraph 2(a) focuses more directly on the protection against child abuse. Paragraphs 2(b) and 2 (c) aim at providing protection against behaviour that, while not necessarily creating harm to the 'child' depicted in the material, as there might not be a real child, might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favouring child abuse.

103. The term 'without right' does not exclude legal defences, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Accordingly, the term 'without right' allows a Party to take into account fundamental rights, such as freedom of thought, expression and privacy. In addition, a Party may provide a defence in respect of conduct related to "pornographic material" having an artistic, medical, scientific or similar merit. In relation to paragraph 2(b), the reference to 'without right' could also allow, for example, that a Party may provide that a person is relieved of criminal responsibility if it is established that the person depicted is not a minor in the sense of this provision.

104. Paragraph 3 defines the term 'minor' in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a 'child' in the UN Convention on the Rights of the Child (Article 1). It was considered an important policy matter to set a uniform international standard regarding age. It should be noted that the age refers to the use of (real or fictitious) children as sexual objects, and is separate from the age of consent for sexual relations. Nevertheless, recognising that certain States require a lower age-limit in national legislation regarding child pornography, the last phrase of paragraph 3 allows Parties to require a different age-limit, provided it is not less than 16 years.

105. This article lists different types of illicit acts related to child pornography which, as in articles 2 - 8, Parties are obligated to criminalise if committed "intentionally." Under this standard, a person is not liable unless he has an intent to offer, make available, distribute, transmit, produce or possess child pornography. Parties may adopt a more specific standard (see, for example, applicable European Community law in relation to service provider liability), in which case that standard would govern. For example, liability may be imposed if there is "knowledge and control" over the information which is transmitted or stored. It is not sufficient, for example, that a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.

106. Paragraph 4 permits Parties to make reservations regarding paragraph 1(d) and (e), and paragraph 2(b) and (c). The right not to apply these sections of the provision may be made in part or in whole. Any such reservation should be declared to the Secretary General of the Council of Europe at the time of signature or when depositing the Party's instruments of ratification, acceptance, approval or accession, in accordance with Article 42.

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

Offences related to infringements of copyright and related rights (Article 10)

107. Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet, which cause concern both to copyright holders and those who work professionally with computer networks. The reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder, are extremely frequent. Such protected works include literary, photographic, musical, audio-visual and other works. The ease with which unauthorised copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks made it necessary to include provisions on criminal law sanctions and enhance international co-operation in this field.

108. Each Party is obliged to criminalise wilful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale". Paragraph 1 provides for criminal sanctions against infringements of copyright by means of a computer system. Infringement of copyright is already an offence in almost all States. Paragraph 2 deals with the infringement of related rights by means of a computer system.

109. Infringement of both copyright and related rights is as defined under the law of each Party and pursuant to the obligations the Party has undertaken in respect of certain international instruments. While each Party is required to establish as criminal offences those infringements, the precise manner in which such infringements are defined under domestic law may vary from State to State. However, criminalisation obligations under the Convention do not cover intellectual property infringements other that those explictly addressed in Article 10 and thus exclude patent or trademark-related violations.

110. With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention.

111. The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty had not entered into force at the time of concluding the present Convention. These treaties are nevertheless important as they significantly update the international protection for intellectual

property (especially with regard to the new right of 'making available' of protected material 'on demand' over the Internet) and improve the means to fight violations of intellectual property rights worldwide. However it is understood that the infringements of rights established by these treaties need not be criminalised under the present Convention until these treaties have entered into force with respect to a Party.

112. The obligation to criminalise infringements of copyright and related rights pursuant to obligations undertaken in international instruments does not extend to any moral rights conferred by the named instruments (such as in Article 6bis of the Bern Convention and in Article 5 of the WIPO Copyright Treaty).

113. Copyright and related rights offences must be committed "wilfully" for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term "wilfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement (Article 61), governing the obligation to criminalise copyright violations.

114. The provisions are intended to provide for criminal sanctions against infringements 'on a commercial scale' and by means of a computer system. This is in line with Article 61 of the TRIPS Agreement which requires criminal sanctions in copyright matters only in the case of "piracy on a commercial scale". However, Parties may wish to go beyond the threshold of "commercial scale" and criminalise other types of copyright infringement as well.

115. The term "without right" has been omitted from the text of this article as redundant, since the term "infringement" already denotes use of the copyrighted material without authorisation. The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

116. Paragraph 3 allows Parties not to impose criminal liability under paragraphs 1 and 2 in "limited circumstances" (e.g. parallel imports, rental rights), as long as other effective remedies, including civil and/or administrative measures, are available. This provision essentially allows Parties a limited exemption from the obligation to impose criminal liability, provided that they do not derogate from obligations under Article 61 of the TRIPS Agreement, which is the minimum pre-existing criminalisation requirement.

117. This article shall in no way be interpreted to extend the protection granted to authors, film producers, performers, producers of phonograms, broadcasting organisations or other right holders to persons that do not meet the criteria for eligibility under domestic law or international agreement.

Title 5 - Ancillary liability and sanctions

Attempt and aiding or abetting (Article 11)

118. The purpose of this article is to establish additional offences related to attempt and aiding or abetting the commission of the offences defined in the Convention. As discussed further below, it is not required that a Party criminalise the attempt to commit each offence established in the Convention.

119. Paragraph 1 requires Parties to establish as criminal offences aiding or abetting the commission of any of the offences under Articles 2-10. Liability arises for aiding or abetting where the person who commits a crime established in the Convention is aided by another person who also intends that the crime be committed. For example, although the transmission of harmful content data or malicious code through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section. Thus, there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision.

120. With respect to paragraph 2 on attempt, some offences defined in the Convention, or elements of these offences, were considered to be conceptually difficult to attempt (for example, the elements of offering or making available of child pornography). Moreover, some legal systems limit the offences for which the attempt is punished. Accordingly, it is only required that the attempt be criminalised with respect to offences established in accordance with Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c).

121. As with all the offences established in accordance with the Convention, attempt and aiding or abetting must be committed intentionally.

122. Paragraph 3 was added to address the difficulties Parties may have with paragraph 2, given the widely varying concepts in different legislations and despite the effort in paragraph 2 to exempt certain aspects from the provision on attempt. A Party may declare that it reserves the right not to apply paragraph 2 in part or in whole. This means that any Party making a reservation as to that provision will have no obligation to criminalise attempt at all, or may select the offences or parts of offences to which it will attach criminal sanctions in relation to attempt. The reservation aims at enabling the widest possible ratification of the Convention while permitting Parties to preserve some of their fundamental legal concepts.

Corporate liability (Article 12)

123. Article 12 deals with the liability of legal persons. It is consistent with the current legal trend to recognise corporate liability. It is intended to impose liability on corporations, associations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 also contemplates liability where such a leading person fails to supervise or control an employee or an agent of the legal person, where such failure facilitates the commission by that employee or agent of one of the offences established in the Convention.

124. Under paragraph 1, four conditions need to be met for liability to attach. First, one of the offences described in the Convention must have been committed. Second, the offence must have been committed for the benefit of the legal person. Third, a person who has a leading position must have committed the offence (including aiding and abetting). The term "person who has a leading position" refers to a natural person who has a high position in the organisation, such as a director. Fourth, the person who has a leading position must have acted on the basis of one of these powers - a power of representation or an authority to take decisions or to exercise control - which demonstrate that such a physical person acted within the scope of his or her authority to engage the liability of the legal person. In sum, paragraph 1 obligates Parties to have the ability to impose liability on the legal person only for offences committed by such leading persons.

125. In addition, Paragraph 2 obligates Parties to have the ability to impose liability upon a legal

person where the crime is committed not by the leading person described in paragraph 1, but by another person acting under the legal person's authority, i.e., one of its employees or agents acting within the scope of their authority. The conditions that must be fulfilled before liability can attach are that (1) an offence has been committed by such an employee or agent of the legal person, (2) the offence has been committed for the benefit of the legal person; and (3) the commission of the offence has been made possible by the leading person having failed to supervise the employee or agent. In this context, failure to supervise should be interpreted to include failure to take appropriate and reasonable measures to prevent employees or agents from committing criminal activities on behalf of the legal person. Such appropriate and reasonable measures could be determined by various factors, such as the type of the business, its size, the standards or the established business best practices, etc. This should not be interpreted as requiring a general surveillance regime over employee communications (see also paragraph 54). A service provider does not incur liability by virtue of the fact that a crime was committed on its system by a customer, user or other third person, because the term "acting under its authority" applies exclusively to employees and agents acting within the scope of their authority.

126. Liability under this Article may be criminal, civil or administrative. Each Party has the flexibility to choose to provide for any or all of these forms of liability, in accordance with the legal principles of each Party, as long as it meets the criteria of Article 13, paragraph 2, that the sanction or measure be "effective, proportionate and dissuasive" and includes monetary sanctions.

127. Paragraph 4 clarifies that corporate liability does not exclude individual liability.

Sanctions and measures (Article 13)

128. This article is closely related to Articles 2-11, which define various computer- or computer-related crimes that should be made punishable under criminal law. In accordance with the obligations imposed by those articles, this provision obliges the Contracting Parties to draw consequences from the serious nature of these offences by providing for criminal sanctions that are 'effective, proportionate and dissuasive' and, in the case of natural persons, include the possibility of imposing prison sentences.

129. Legal persons whose liability is to be established in accordance with Article 12 shall also be subject to sanctions that are 'effective, proportionate and dissuasive', which can be criminal, administrative or civil in nature. Contracting Parties are compelled, under paragraph 2, to provide for the possibility of imposing monetary sanctions on legal persons.

130. The article leaves open the possibility of other sanctions or measures reflecting the seriousness of the offences, for example, measures could include injunction or forfeiture. It leaves to the Parties the discretionary power to create a system of criminal offences and sanctions that is compatible with their existing national legal systems.

Section 2 - Procedural law

131. The articles in this Section describe certain procedural measures to be taken at the national level for the purpose of criminal investigation of the offences established in Section 1, other criminal offences committed by means of a computer system and the collection of evidence in electronic form of a criminal offence. In accordance with Article 39, paragraph 3, nothing in the Convention requires or invites a Party to establish powers or procedures other than those contained in this Convention, nor precludes a Party from doing so.

132. The technological revolution, which encompasses the "electronic highway" where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the sphere of criminal law and criminal procedure. The ever-expanding network of communications opens new doors for criminal activity in respect of both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. Equally, safeguards should also be adapted or developed to keep abreast of the new technological environment and new procedural powers.

133. One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation.

134. The Convention adapts traditional procedural measures, such as search and seizure, to the new technological environment. Additionally, new measures have been created, such as expedited preservation of data, in order to ensure that traditional measures of collection, such as search and seizure, remain effective in the volatile technological environment. As data in the new technological environment is not always static, but may be flowing in the process of communication, other traditional collection procedures relevant to telecommunications, such as real-time collection of traffic data and interception of content data, have also been adapted in order to permit the collection of electronic data that is in the process of communication. Some of these measures are set out in Council of Europe Recommendation No. R (95) 13 on problems of criminal procedural law connected with information technology.

135. All the provisions referred to in this Section aim at permitting the obtaining or collection of data for the purpose of specific criminal investigations or proceedings. The drafters of the present Convention discussed whether the Convention should impose an obligation for service providers to routinely collect and retain traffic data for a certain fixed period of time, but did not include any such obligation due to lack of consensus.

136. The procedures in general refer to all types of data, including three specific types of computer data (traffic data, content data and subscriber data), which may exist in two forms (stored or in the process of communication). Definitions of some of these terms are provided in Articles 1 and 18. The applicability of a procedure to a particular type or form of electronic data depends on the nature and form of the data and the nature of the procedure, as specifically described in each article.

137. In adapting traditional procedural laws to the new technological environment, the question of appropriate terminology arises in the provisions of this section. The options included maintaining traditional language ('search' and 'seize'), using new and more technologically oriented computer terms ('access' and 'copy'), as adopted in texts of other international fora on the subject (such as the G8 High Tech Crime Subgroup), or employing a compromise of mixed language ('search or similarly access', and 'seize or similarly secure'). As there is a need to reflect the evolution of concepts in the electronic environment, as well as identify and maintain their traditional roots, the flexible approach of allowing States to use either the old notions of "search and seizure" or the new notions of "access and copying" is employed.

138. All the articles in the Section refer to "competent authorities" and the powers they shall be

granted for the purposes of specific criminal investigations or proceedings. In certain countries, only judges have the power to order or authorise the collection or production of evidence, while in other countries prosecutors or other law enforcement officers are entrusted with the same or similar powers. Therefore, 'competent authority' refers to a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

Title 1 – Common provisions

139. The Section begins with two provisions of a general nature that apply to all the articles relating to procedural law.

Scope of procedural provisions (Article 14)

140. Each State Party is obligated to adopt such legislative and other measures as may be necessary, in accordance with its domestic law and legal framework, to establish the powers and procedures described in this Section for the purpose of "specific criminal investigations or proceedings."

141. Subject to two exceptions, each Party shall apply the powers and procedures established in accordance with this Section to: (i) criminal offences established in accordance with Section 1 of the Convention; (ii) other criminal offences committed by means of a computer system; and (iii) the collection of evidence in electronic form of a criminal offence. Thus, for the purpose of specific criminal investigations or proceedings, the powers and procedures referred to in this Section shall be applied to offences established in accordance with the Convention, to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence. This ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of the powers and procedures set out in this Section. It ensures an equivalent or parallel capability for the obtaining or collection of computer data as exists under traditional powers and procedures for non-electronic data. The Convention makes it explicit that Parties should incorporate into their laws the possibility that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted.

142. There are two exceptions to this scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law. Many States limit the power of interception of oral communications or telecommunications to a range of serious offences, in recognition of the privacy of oral communications and telecommunications and the intrusiveness of this investigative measure. Likewise, this Convention only requires Parties to establish interception powers and procedures in relation to content data of specified computer communications in respect of a range of serious offences to be determined by domestic law.

143. Second, a Party may reserve the right to apply the measures in Article 20 (real-time collection of traffic data) only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories is not more restricted than the range of offences to which it applies the interception measures referred to in Article 21. Some States consider the collection of traffic data as being equivalent to the collection of content data in terms of privacy and intrusiveness. The right of reservation would permit these States to limit the

application of the measures to collect traffic data, in real-time, to the same range of offences to which it applies the powers and procedures of real-time interception of content data. Many States, however, do not consider the interception of content data and the collection of traffic data to be equivalent in terms of privacy interests and degree of intrusiveness, as the collection of traffic data alone does not collect or disclose the content of the communication. As the real-time collection of traffic data can be very important in tracing the source or destination of computer communications (thus, assisting in identifying criminals), the Convention invites Parties that exercise the right of reservation to limit their reservation so as to enable the broadest application of the powers and procedures provided to collect, in real-time, traffic data.

144. Paragraph (b) provides a reservation for countries which, due to existing limitations in their domestic law at the time of the Convention's adoption, cannot intercept communications on computer systems operated for the benefit of a closed group of users and which do not use public communications networks nor are they connected with other computer systems. The term "closed group of users" refers, for example, to a set of users that is limited by association to the service provider, such as the employees of a company for which the company provides the ability to communicate amongst themselves using a computer network. The term "not connected with other computer systems" means that, at the time an order under Articles 20 or 21 would be issued, the system on which communications are being transmitted does not have a physical or logical connection to another computer network. The term "does not employ public communications networks" excludes systems that use public computer networks (including the Internet), public telephone networks or other public telecommunications facilities in transmitting communications, whether or not such use is apparent to the users.

Conditions and safeguards (Article 15)

145. The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments. These instruments include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005 (4), 009, 046, 114, 117 and 177), in respect of European States that are Parties to them. It also includes other applicable human rights instruments in respect of States in other regions of the world (e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights) which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.

146. Another safeguard in the convention is that the powers and procedures shall "incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures. Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.

147. Without limiting the types of conditions and safeguards that could be applicable, the Convention requires specifically that such conditions and safeguards include, as appropriate in view of the nature of the power or procedure, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards. As stated in Paragraph 215, Parties should clearly apply conditions and safeguards such as these with respect to interception, given its intrusiveness. At the same time, for example, such safeguards need not apply equally to preservation. Other safeguards that should be addressed under domestic law include the right against self-incrimination, and legal privileges and specificity of individuals or places which are the object of the application of the measure.

148. With respect to the matters discussed in paragraph 3, of primary importance is consideration of the "public interest", in particular the interests of "the sound administration of justice". To the extent consistent with the public interest, Parties should consider other factors, such as the impact of the power or procedure on "the rights, responsibilities and legitimate interests" of third parties, including service providers, incurred as a result of the enforcement measures, and whether appropriate means can be taken to mitigate such impact. In sum, initial consideration is given to the sound administration of justice and other public interests (e.g. public safety and public health and other interests, including the interests of victims and the respect for private life). To the extent consistent with the public interest, consideration would ordinarily also be given to such issues as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under this Chapter, or protection of proprietary interests.

Title 2 – Expedited preservation of stored computer data

149. The measures in Articles 16 and 17 apply to stored data that has already been collected and retained by data-holders, such as service providers. They do not apply to the real-time collection and retention of future traffic data or to real-time access to the content of communications. These issues are addressed in Title 5.

150. The measures described in the articles operate only where computer data already exists and is currently being stored. For many reasons, computer data relevant for criminal investigations may not exist or no longer be stored. For example, accurate data may not have been collected and retained, or if collected was not maintained. Data protection laws may have affirmatively required the destruction of important data before anyone realised its significance for criminal proceedings. Sometimes there may be no business reason for the collection and retention of data, such as where customers pay a flat rate for services or the services are free. Article 16 and 17 do not address

these problems.

151. "Data preservation" must be distinguished from "data retention". While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe.

152. Articles 16 and 17 refer only to data preservation, and not data retention. They do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities. The preservation measures apply to computer data that "has been stored by means of a computer system", which presupposes that the data already exists, has already been collected and is stored. Furthermore, as indicated in Article 14, all of the powers and procedures required to be established in Section 2 of the Convention are 'for the purpose of specific criminal investigations or proceedings', which limits the application of the measures to an investigation in a particular case. Additionally, where a Party gives effect to preservation measures by means of an order, this order is in relation to "specified stored computer data in the person's possession or control" (paragraph 2). The articles, therefore, provide only for the power to require preservation of existing stored data, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings.

153. The obligation to ensure preservation of data is not intended to require Parties to restrict the offering or use of services that do not routinely collect and retain certain types of data, such as traffic or subscriber data, as part of their legitimate business practices. Neither does it require them to implement new technical capabilities in order to do so, e.g. to preserve ephemeral data, which may be present on the system for such a brief period that it could not be reasonably preserved in response to a request or an order.

154. Some States have laws that require that certain types of data, such as personal data, held by particular types of holders must not be retained and must be deleted if there is no longer a business purpose for the retention of the data. In the European Union, the general principle is implemented by Directive 95/46/EC and, in the particular context of the telecommunications sector, Directive 97/66/EC. These directives establish the obligation to delete data as soon as its storage is no longer necessary. However, member States may adopt legislation to provide for exemptions when necessary for the purpose of the prevention, investigation or prosecution of criminal offences. These directives do not prevent member States of the European Union from establishing powers and procedures under their domestic law to preserve specified data for specific investigations.

155. Data preservation is for most countries an entirely new legal power or procedure in domestic law. It is an important new investigative tool in addressing computer and computer-related crime, especially crimes committed through the Internet. First, because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained. One method of preserving its integrity is for competent authorities to search or similarly access and seize or similarly secure the data. However, where the custodian of the data is trustworthy, such as a reputable business, the integrity of the data can be secured more quickly by means of an order to preserve the data. For legitimate businesses, a preservation order may also be less

disruptive to its normal activities and reputation than the execution of a search and seizure of its premises. Second, computer and computer-related crimes are committed to a great extent as a result of the transmission of communications through the computer system. These communications may contain illegal content, such as child pornography, computer viruses or other instructions that cause interference with data or the proper functioning of the computer system, or evidence of the commission of other crimes, such as drug trafficking or fraud. Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required (see further explanation on the importance of traffic data below under Article 17). Third, where these communications contain illegal content or evidence of criminal activity and copies of such communications are retained by service providers, such as e-mail, the preservation of these communications is important in order to ensure that critical evidence is not lost. Obtaining copies of these past communications (e.g., stored e-mail that has been sent or received) can reveal evidence of criminality.

156. The power of expedited preservation of computer data is intended to address these problems. Parties are therefore required to introduce a power to order the preservation of specified computer data as a provisional measure, whereby data will be preserved for a period of time as long as necessary, up to a maximum of 90 days. A Party may provide for subsequent renewal of the order. This does not mean that the data is disclosed to law enforcement authorities at the time of preservation. For this to happen, an additional measure of disclosure or a search has to be ordered. With respect to disclosure to law enforcement of preserved data, see paragraphs 152 and 160.

157. It is also important that preservation measures exists at the national level in order to enable Parties to assist one another at the international level with expedited preservation of stored data located in their territory. This will help to ensure that critical data is not lost during often time-consuming traditional mutual legal assistance procedures that enable the requested Party to actually obtain the data and disclose it to the requesting Party.

Expedited preservation of stored computer data (Article 16)

158. Article 16 aims at ensuring that national competent authorities are able to order or similarly obtain the expedited preservation of specified stored computer-data in connection with a specific criminal investigation or proceeding.

159. 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. It requires that it be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be 'frozen' (i.e. rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users. The person to whom the order is addressed may, depending on the exact specifications of the order, still access the data. The article does not specify how data should be preserved. It is left to each Party to determine the appropriate manner of preservation and whether, in some appropriate cases, preservation of the data should also entail its 'freezing'.

160. The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor). In some States, preservation orders do not exist in their procedural law, and data can only be preserved and obtained through search and seizure or production order. Flexibility is intended by the use of the phrase 'or otherwise obtain' to permit these States to implement this article by the use of these means. However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the

order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases.

161. The power to order or similarly obtain the expeditious preservation of specified computer data applies to any type of stored computer data. This can include any type of data that is specified in the order to be preserved. It can include, for example, business, health, personal or other records. The measures are to be established by Parties for use "in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification." This can include situations where the data is subject to a short period of retention, such as where there is a business policy to delete the data after a certain period of time or the data is ordinarily deleted when the storage medium is used to record other data. It can also refer to the nature of the custodian of the data or the insecure manner in which the data is stored. However, if the custodian were untrustworthy, it would be more secure to effect preservation by means of search and seizure, rather than by means of an order that could be disobeyed. A specific reference to "traffic data" is made in paragraph 1 in order to signal the provisions particular applicability to this type of data, which if collected and retained by a service provider, is usually held for only a short period of time. The reference to "traffic data" also provides a link between the measures in Article 16 and 17.

162. Paragraph 2 specifies that where a Party gives effect to preservation by means of an order, the order to preserve is in relation to "specified stored computer data in the person's possession or control". Thus, the stored data may actually be in the possession of the person or it may be stored elsewhere but subject to the control of this person. The person who receives the order is obliged "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure." The domestic law of a Party should specify a maximum period of time for which data, subject to an order, must be preserved, and the order should specify the exact period of time that the specified data is to be preserved. The period of time should be as long as necessary, up to a maximum of 90 days, to permit the competent authorities to undertake other legal measures, such as search and seizure, or similar access or securing, or the issuance of a production order, to obtain the disclosure of the data. A Party may provide for subsequent renewal of the production order. In this context, reference should be made to Article 29, which concerns a mutual assistance request to obtain the expeditious preservation of data stored by means of a computer system. That article specifies that preservation effected in response to a mutual assistance request "shall be for a period not less than 60 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."

163. Paragraph 3 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This requires Parties to introduce confidentiality measures in respect of expedited preservation of stored data, and a time limit in respect of the period of confidentiality. This measure accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. For law enforcement authorities, the expedited preservation of data forms part of initial investigations and, therefore, covertness may be important at this stage. Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order that other persons do not attempt to tamper with or delete the data. For the person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that the preservation measure has been undertaken helps to protect the

privacy of the data subject or other persons who may be mentioned or identified in that data.

164. In addition to the limitations set out above, the powers and procedures referred to in Article 16 are also subject to the conditions and safeguards provided in Articles 14 and 15.

Expedited preservation and partial disclosure of traffic data (Article 17)

165. This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service providers were involved in the transmission of specified communications. "Traffic data" is defined in Article 1.

166. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data (see discussion related to preservation, above).

167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

168. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service providers. The article does not specify the means by which this may be achieved, leaving it to domestic law to determine a means that is consistent with its legal and economic system. One means to achieve expeditious preservation would be for competent authorities to serve expeditiously a separate preservation order on each service provider. Nevertheless, obtaining a series of separate orders can be unduly time consuming. A preferred alternative could be to obtain a single order, the scope of which however would apply to all service providers that were identified subsequently as being involved in the transmission of the specific communication. This comprehensive order could be served sequentially on each service provider identified. Other possible alternatives could involve the participation of service providers. For example, requiring a service provider that was served with an order to notify the next service provider in the chain of the existence and terms of the preservation order. This notice could, depending on domestic law, have the effect of either permitting the other service provider to preserve voluntarily the relevant traffic data, despite any obligations to delete it, or mandating the preservation of the relevant

traffic data. The second service provider could similarly notify the next service provider in the chain.

169. As traffic data is not disclosed to law enforcement authorities upon service of a preservation order to a service provider (but only obtained or disclosed subsequently upon the taking of other legal measures), these authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted. The competent authorities should specify clearly the type of traffic data that is required to be disclosed. Receipt of this information would enable the competent authorities to determine whether to take preservation measures with respect to the other service providers. In this way, the investigating authorities can trace the communication back to its origin, or forward to its destination, and identify the perpetrator or perpetrators of the specific crime being investigated. The measures in this article are also subject to the limitations, conditions and safeguards provided in Articles 14 and 15.

Title 3 – Production order

Production order (Article 18)

170. Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations.

171. A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

172. The production order refers to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the

ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.

174. The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases.

175. A further consideration for Parties is the possible inclusion of measures concerning confidentiality. The provision does not contain a specific reference to confidentiality, in order to maintain the parallel with the non-electronic world where confidentiality is not imposed in general regarding production orders. However, in the electronic, particularly on-line, world a production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data. Confidentiality could be essential for the success of the investigation.

176. With respect to the modalities of production, Parties could establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order. This could include reference to a time period within which disclosure must be made, or to form, such as that the data or information be provided in "plain text", on-line or on a paper print-out or on a diskette.

177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special

provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

178. In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address). Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.

179. Therefore, subscriber information includes various types of information about the use of a service and the user of that service. With respect to the use of the service, the term means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service. The term 'technical provisions' includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks).

180. Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider. It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement. This latter information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment (on the basis of the information provided according to the service agreement or arrangement) can be instrumental to an investigation.

181. However, this article should not be understood as to impose an obligation on service providers to keep records of their subscribers, nor would it require service providers to ensure the correctness of such information. Thus, a service provider is not obliged to register identity information of users of so-called prepaid cards for mobile telephone services. Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.

182. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not

authorise Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining.

183. The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services.

Title 4 – Search and seizure of stored computer data

Search and seizure of stored computer data (Article 19)

184. This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data *per se* will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data.

185. In the traditional search environment concerning documents or records, a search involves gathering evidence that has been recorded or registered in the past in tangible form, such as ink on paper. The investigators search or inspect such recorded data, and seize or physically take away the tangible record. The gathering of data takes place during the period of the search and in respect of data that exists at that time. The precondition for obtaining legal authority to undertake a search is the existence of grounds to believe, as prescribed by domestic law and human rights safeguards, that such data exists in a particular location and will afford evidence of a specific criminal offence.

186. With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain. For example, the gathering of the data occurs during the period of the search and in respect of data that exists at that time. The preconditions for obtaining legal authority to undertake a search remain the same. The degree of belief required for obtaining legal authorisation to search is not any different whether the data is in tangible form or in electronic form. Likewise, the belief and the search are in respect of data that already exists and that will afford evidence of a specific offence.

187. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form, on a physical medium (e.g., diskette), before the tangible medium containing the copy can be seized and taken away. In the latter two situations, where such copies of the data are made, a copy of the data remains in the computer system or storage device. Domestic law should provide for a power to make such copies. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or

connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations.

188. Paragraph 1 requires Parties to empower law enforcement authorities to access and search computer data, which is contained either within a computer system or part of it (such as a connected data storage device), or on an independent data storage medium (such as a CD-ROM or diskette). As the definition of "computer system" in article 1 refers to "any device or a group of inter-connected or related devices", paragraph 1 concerns the search of a computer system and its related components that can be considered together as forming one distinct computer system (e.g., a PC together with a printer and related storage devices, or a local area network). Sometimes data that is physically stored in another system or storage device can be legally accessed through the searched computer system by establishing a connection with other distinct computer systems. This situation, involving linkages with other computer systems by means of telecommunication networks within the same territory (e.g., wide area network or Internet), is addressed at paragraph 2.

189. Although search and seizure of a "computer-data storage medium in which computer data may be stored" (paragraph 1 (b)) may be undertaken by use of traditional search powers, often the execution of a computer search requires both the search of the computer system and any related computer-data storage medium (e.g., diskettes) in the immediate vicinity of the computer system. Due to this relationship, a comprehensive legal authority is provided in paragraph 1 to encompass both situations.

190. Article 19 applies to stored computer data. In this respect, the question arises whether an unopened e-mail message waiting in the mailbox of an ISP until the addressee will download it to his or her computer system, has to be considered as stored computer data or as data in transfer. Under the law of some Parties, that e-mail message is part of a communication and therefore its content can only be obtained by applying the power of interception, whereas other legal systems consider such message as stored data to which article 19 applies. Therefore, Parties should review their laws with respect to this issue to determine what is appropriate within their domestic legal systems.

191. Reference is made to the term 'search or similarly access'. The use of the traditional word 'search' conveys the idea of the exercise of coercive power by the State, and indicates that the power referred to in this article is analogous to traditional search. 'Search' means to seek, read, inspect or review data. It includes the notions of searching for data and searching of (examining) data. On the other hand, the word 'access' has a neutral meaning, but it reflects more accurately computer terminology. Both terms are used in order to marry the traditional concepts with modern terminology.

192. The reference to 'in its territory' is a reminder that this provision, as all the articles in this Section, concern only measures that are required to be taken at the national level.

193. Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory'.

194. The Convention does not prescribe how an extension of a search is to be permitted or undertaken. This is left to domestic law. Some examples of possible conditions are: empowering the judicial or other authority which authorised the computer search of a specific computer system, to authorise the extension of the search or similar access to a connected system if he or she has grounds to believe (to the degree required by national law and human rights safeguards) that the connected computer system may contain the specific data that is being sought; empowering the investigative authorities to extend an authorised search or similar access of a specific computer system to a connected computer system where there are similar grounds to believe that the specific data being sought is stored in the other computer system; or exercising search or similar access powers at both locations in a co-ordinated and expeditious manner. In all cases the data to be searched must be lawfully accessible from or available to the initial computer system.

195. This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation.

196. Paragraph 3 addresses the issues of empowering competent authorities to seize or similarly secure computer data that has been searched or similarly accessed under paragraphs 1 or 2. This includes the power of seizure of computer hardware and computer-data storage media. In certain cases, for instance when data is stored in unique operating systems such that it cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. This may also be necessary when the data carrier has to be examined in order to retrieve from it older data which was overwritten but which has, nevertheless, left traces on the data carrier.

197. In this Convention, 'seize' means to take away the physical medium upon which data or information is recorded, or to make and retain a copy of such data or information. 'Seize' includes the use or seizure of programmes needed to access the data being seized. As well as using the traditional term 'seize', the term 'similarly secure' is included to reflect other means by which intangible data is removed, rendered inaccessible or its control is otherwise taken over in the computer environment. Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data.

198. The rendering inaccessible of data can include encrypting the data or otherwise technologically denying anyone access to that data. This measure could usefully be applied in situations where danger or social harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography. The term 'removal' is intended to express the idea that while the data is removed or rendered inaccessible, it is not destroyed, but continues to exist. The suspect is temporarily deprived of the data, but it can be returned following the outcome of the criminal investigation or proceedings.

199. Thus, seize or similarly secure data has two functions: 1) to gather evidence, such as by copying the data, or 2) to confiscate data, such as by copying the data and subsequently rendering the original version of the data inaccessible or by removing it. The seizure does not imply a final deletion of the seized data.

200. Paragraph 4 introduces a coercive measure to facilitate the search and seizure of computer data. It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted. This provision, therefore, allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure.

201. This power is not only of benefit to the investigating authorities. Without such co-operation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.

202. The information that can be ordered to be provided is that which is necessary to enable the undertaking of the search and seizure, or the similarly accessing or securing. The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable provision may include disclosing a password or other security measure to the investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such case, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities.

203. Under paragraph 5 of this article, the measures are subject to conditions and safeguards provided for under domestic law on the basis of Article 15 of this Convention. Such conditions may include provisions relating to the engagement and financial compensation of witnesses and experts.

204. The drafters discussed further in the frame of paragraph 5 if interested parties should be notified of the undertaking of a search procedure In the on-line world it may be less apparent that data has been searched and seized (copied) than that a seizure in the off-line world took place, where seized objects will be physically missing. The laws of some Parties do not provide for an obligation to notify in the case of a traditional search. For the Convention to require notification in respect of a computer search would create a discrepancy in the laws of these Parties. On the other hand, some Parties may consider notification as an essential feature of the measure, in order to maintain the distinction between computer search of stored data (which is generally not intended to be a surreptitious measure) and interception of flowing data (which is a surreptitious measure, see Articles 20 and 21). The issue of notification, therefore, is left to be determined by domestic law. If Parties consider a system of mandatory notification of persons concerned, it should be borne in mind that such notification may prejudice the investigation. If such a risk exists, postponement of the notification should be considered.

Title 5 – Real-time collection of computer data

205. Articles 20 and 21 provide for the real-time collection of traffic data and the real-time interception of content data associated with specified communications transmitted by a computer

system. The provisions address the real-time collection and real-time interception of such data by competent authorities, as well as their collection or interception by service providers. Obligations of confidentiality are also addressed.

206. Interception of telecommunications usually refers to traditional telecommunications networks. These networks can include cable infrastructures, whether wire or optical cable, as well as inter-connections with wireless networks, including mobile telephone systems and microwave transmission systems. Today, mobile communications are facilitated also by a system of special satellite networks. Computer networks may also consist of an independent fixed cable infrastructure, but are more frequently operated as a virtual network by connections made through telecommunication infrastructures, thus permitting the creation of computer networks or linkages of networks that are global in nature. The distinction between telecommunications and computer communications, and the distinctiveness between their infrastructures, is blurring with the convergence of telecommunication and information technologies. Thus, the definition of 'computer system' in article 1 does not restrict the manner by which the devices or group of devices may be inter-connected. Articles 20 and 21, therefore, apply to specified communications transmitted by means of a computer system, which could include transmission of the communication through telecommunication networks before it is received by another computer system.

207. Articles 20 and 21 do not make a distinction between a publicly or a privately owned telecommunication or computer system or to the use of systems and communication services offered to the public or to closed user groups or private parties. The definition of 'service provider' in Article 1 refers to public and private entities that provide to users of their services the ability to communicate by means of a computer system.

208. This Title governs the collection of evidence contained in currently generated communications, which are collected at the time of the communication (i.e., 'real time'). The data are intangible in form (e.g., in the form of transmissions of voice or electronic impulses). The flow of the data is not significantly interfered with by the collection, and the communication reaches its intended recipient. Instead of a physical seizure of the data, a recording (i.e., a copy) is made of the data being communicated. The collection of this evidence takes place during a certain period of time. A legal authority to permit the collection is sought in respect of a future event (i.e., a future transmission of data).

209. The type of data that can be collected is of two types: traffic data and content data. 'Traffic data' is defined in Article 1 d to mean any computer data relating to a communication made by means of a computer system, which is generated by the computer system and which formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size and duration or the type of service. 'Content data' is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).

210. In many States, a distinction is made between the real-time interception of content data and real-time collection of traffic data in terms of both the legal prerequisites required to authorise such investigative measure and the offences in respect of which this measure can be employed. While recognising that both types of data may have associated privacy interests, many States consider that the privacy interests in respect of content data are greater due to the nature of the communication content or message. Greater limitations may be imposed with respect to the real-time collection of content data than traffic data. To assist in recognising this distinction for these

States, the Convention, while operationally acknowledging that the data is collected or recorded in both situations, refers normatively in the titles of the articles to the collection of traffic data as 'real-time collection' and the collection of content data as 'real-time interception'.

211. In some States existing legislation makes no distinction between the collection of traffic data and the interception of content data, either because no distinction has been made in the law regarding differences in privacy interests or the technological collection techniques for both measures are very similar. Thus, the legal prerequisites required to authorise the undertaking of the measures, and the offences in respect of which the measures can be employed, are the same. This situation is also recognised in the Convention by the common operational use of the term 'collect or record' in the actual text of both Articles 20 and 21.

212. With respect to the real-time interception of content data, the law often prescribes that the measure is only available in relation to the investigation of serious offences or categories of serious offences. These offences are identified in domestic law as serious for this purpose often by being named in a list of applicable offences or by being included in this category by reference to a certain maximum sentence of incarceration that is applicable to the offence. Therefore, with respect to the interception of content data, Article 21 specifically provides that Parties are only required to establish the measure 'in relation to a range of serious offences to be determined by domestic law'.

213. Article 20, concerning the collection of traffic data, on the other hand, is not so limited and in principle applies to any criminal offence covered by the Convention. However, Article 14, paragraph 3, provides that a Party may reserve the right to apply the measure only to offences or categories of offences specified in the reservation, provided that the range of offences or categories of offences is not more restricted than the range of offences to which it applies the measure of interception of content data. Nevertheless, where such a reservation is taken, the Party shall consider restricting such reservation so as to enable the broadest range of application of the measure of collection of traffic data.

214. For some States, the offences established in the Convention would normally not be considered serious enough to permit interception of content data or, in some cases, even the collection of traffic data. Nevertheless, such techniques are often crucial for the investigation of some of the offences established in the Convention, such as those involving illegal access to computer systems, and distribution of viruses and child pornography. The source of the intrusion or distribution, for example, cannot be determined in some cases without real-time collection of traffic data. In some cases, the nature of the communication cannot be discovered without real-time interception of content data. These offences, by their nature or the means of transmission, involve the use of computer technologies. The use of technological means should, therefore, be permitted to investigate these offences. However, due to the sensitivities surrounding the issue of interception of content data, the Convention leaves the scope of this measure to be determined by domestic law. As some countries legally assimilate the collection of traffic data with the interception of content data, a reservation possibility is permitted to restrict the applicability of the former measure, but not to an extent greater than a Party restricts the measure of real-time interception of content data. Nevertheless, Parties should consider applying the two measures to the offences established by the Convention in Section 1 of Chapter II, in order to provide an effective means for the investigation of these computer offences and computer-related offences.

215. The conditions and safeguards regarding the powers and procedures related to real-time interception of content data and real-time collection of traffic data are subject to Articles 14 and 15. As interception of content data is a very intrusive measure on private life, stringent safeguards

are required to ensure an appropriate balance between the interests of justice and the fundamental rights of the individual. In the area of interception, the present Convention itself does not set out specific safeguards other than limiting authorisation of interception of content data to investigations into serious criminal offences as defined in domestic law. Nevertheless, the following important conditions and safeguards in this area, applied in domestic laws, are: judicial or other independent supervision; specificity as to the communications or persons to be intercepted; necessity, subsidiarity and proportionality (e.g. legal predicates justifying the taking of the measure; other less intrusive measures not effective); limitation on the duration of interception; right of redress. Many of these safeguards reflect the European Convention on Human Rights and its subsequent case-law (see judgements in Klass (5), Kruslin (6), Huvig (7), Malone (8), Halford (9), Lambert (10) cases). Some of these safeguards are applicable also to the collection of traffic data in real-time.

Real-time collection of traffic data (Article 20)

216. Often, historical traffic data may no longer be available or it may not be relevant as the intruder has changed the route of communication. Therefore, the real-time collection of traffic data is an important investigative measure. Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings.

217. Traditionally, the collection of traffic data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine the source or destination (e.g., telephone numbers) and related data (e.g., time, date and duration) of various types of illegal communications (e.g., criminal threats and harassment, criminal conspiracy, fraudulent misrepresentations) and of communications affording evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.).

218. Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it also has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography). Likewise, as computers can store vast quantities of data, often of a private nature, the potential for harm, whether economic, social or personal, can be significant if the integrity of this data is interfered with. Furthermore, as the science of computer technology is founded upon the processing of data, both as an end product and as part of its operational function (e.g., execution of computer programs), any interference with this data can have disastrous effects on the proper operation of computer systems. When an illegal distribution of child pornography, illegal access to a computer system or interference with the proper functioning of the computer system or the integrity of data, is committed, particularly from a distance such as through the Internet, it is necessary and crucial to trace the route of the communications back from the victim to the perpetrator. Therefore, the ability to collect traffic data in respect of computer communications is just as, if not more, important as it is in respect of purely traditional telecommunications. This investigative technique can correlate the time, date and source and destination of the suspect's communications with the time of the intrusions into the systems of victims, identify other victims or show links with associates.

219. Under this article, the traffic data concerned must be associated with specified communications in the territory of the Party. The specified 'communications' are in the plural, as traffic data in respect of several communications may need to be collected in order to determine the human source or destination (for example, in a household where several different persons have the use of the same telecommunications facilities, it may be necessary to correlate several communications with the individuals' opportunity to use the computer system). The

communications in respect of which the traffic data may be collected or recorded, however, must be specified. Thus, the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.

220. Subject to paragraph 2, Parties are obliged, under paragraph 1(a) to ensure that their competent authorities have the capacity to collect or record traffic data by technical means. The article does not specify technologically how the collection is to be undertaken, and no obligations in technical terms are defined.

221. In addition, under paragraph 1(b), Parties are obliged to ensure that their competent authorities have the power to compel a service provider to collect or record traffic data or to co-operate and assist the competent authorities in the collection or recording of such data. This obligation regarding service providers is applicable only to the extent that the collection or recording, or co-operation and assistance, is within the existing technical capability of the service provider. The article does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems. However, if their systems and personnel have the existing technical capability to provide such collection, recording, co-operation or assistance, the article would require them to take the necessary measures to engage such capability. For example, the system may be configured in such a manner, or computer programs may already be possessed by the service provider, which would permit such measures to be taken, but they are not ordinarily executed or used in the normal course of the service provider's operation. The article would require the service provider to engage or turn-on these features, as required by law.

222. As this is a measure to be carried out at national level, the measures are applied to the collection or recording of specified communications in the territory of the Party. Thus, in practical terms, the obligations are generally applicable where the service provider has some physical infrastructure or equipment on that territory capable of undertaking the measures, although this need not be the location of its main operations or headquarters. For the purposes of this Convention, it is understood that a communication is in a Party's territory if one of the communicating parties (human beings or computers) is located in the territory or if the computer or telecommunication equipment through which the communication passes is located on the territory.

223. In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a)). Likewise, an obligation under paragraph 1(b)(ii) to co-operate and assist the competent authorities in the collection or recording of traffic data is senseless if the competent authorities are not empowered to collect or record themselves the traffic data. Additionally, in the situation of some local area networks (LANs), where no service provider may be involved, the only way for collection or recording to be carried out would be for the investigating authorities to do it themselves. Both measures in paragraphs 1 (a) and (b) do not have to be used each time, but the availability of both methods is required by the article.

224. This dual obligation, however, posed difficulties for certain States in which the law enforcement authorities were only able to intercept data in telecommunication systems through the assistance of a service provider, or not surreptitiously without at least the knowledge of the service provider. For this reason, paragraph 2 accommodates such a situation. Where a Party, due to the 'established principles of its domestic legal system', cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt a different approach, such as only compelling service providers to provide the necessary technical facilities, to ensure the real-time collection of traffic data by law enforcement authorities. In such case, all of the other limitations regarding territory, specificity of communications and use of technical means still apply.

225. Like real-time interception of content data, real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Interception is surreptitious and must be carried out in such a manner that the communicating parties will not perceive the operation. Service providers and their employees knowing about the interception must, therefore, be under an obligation of secrecy in order for the procedure to be undertaken effectively.

226. Paragraph 3 obligates Parties to adopt such legislative or other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data. This provision not only ensures the confidentiality of the investigation, but it also relieves the service provider of any contractual or other legal obligations to notify subscribers that data about them is being collected. Paragraph 3 may be effected by the creation of explicit obligations in the law. On the other hand, a Party may be able to ensure the confidentiality of the measure on the basis of other domestic legal provisions, such as the power to prosecute for obstruction of justice those persons who aid the criminals by telling them about the measure. Although a specific confidentiality requirement (with effective sanction in case of a breach) is a preferred procedure, the use of obstruction of justice offences can be an alternative means to prevent inappropriate disclosure and, therefore, also suffices to implement this paragraph. Where explicit obligations of confidentiality are created, these shall be subject to the conditions and safeguards as provided in Articles 14 and 15. These safeguards or conditions should impose reasonable time periods for the duration of the obligation, given the surreptitious nature of the investigative measure.

227. As noted above, the privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures, pursuant to Articles 14 and 15.

Interception of content data (Article 21)

228. Traditionally, the collection of content data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine that the communication is of an illegal nature (e.g., the communication constitutes a criminal threat or harassment, a criminal conspiracy or fraudulent misrepresentations) and to collect evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.). Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is

capable of transmitting vast quantities of data, including written text, visual images and sound, it has greater potential for committing crimes involving distribution of illegal content (e.g., child pornography). Many of the computer crimes involve the transmission or communication of data as part of their commission; for example, communications sent to effect an illegal access of a computer system or the distribution of computer viruses. It is not possible to determine in real-time the harmful and illegal nature of these communications without intercepting the content of the message. Without the ability to determine and prevent the occurrence of criminality in progress, law enforcement would merely be left with investigating past and completed crimes where the damage has already occurred. Therefore, the real-time interception of content data of computer communications is just as, if not more, important as is the real-time interception of telecommunications.

229. 'Content data' refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication. It is everything transmitted as part of the communication that is not traffic data.

230. Most of the elements of this article are identical to those of Article 20. Therefore, the comments, above, concerning the collection or recording of traffic data, obligations to co-operate and assist, and obligations of confidentiality apply equally to the interception of content data. Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'.

231. Also, as set forth in the comments above on Article 20, the conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data, or to the search and seizure or similar accessing or securing of stored data.

Section 3 - Jurisdiction

Jurisdiction (Article 22)

232. This Article establishes a series of criteria under which Contracting Parties are obliged to establish jurisdiction over the criminal offences enumerated in Articles 2-11 of the Convention.

233. Paragraph 1 *littera a* is based upon the principle of territoriality. Each Party is required to punish the commission of crimes established in this Convention that are committed in its territory. For example, a Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not.

234. Consideration was given to including a provision requiring each Party to establish jurisdiction over offences involving satellites registered in its name. The drafters decided that such a provision was unnecessary since unlawful communications involving satellites will invariably originate from and/or be received on earth. As such, one of the bases for a Party's jurisdiction set forth in paragraph 1(a) – (c) will be available if the transmission originates or terminates in one of the locations specified therein. Further, to the extent the offence involving a satellite communication is committed by a Party's national outside the territorial jurisdiction of any State, there will be a jurisdictional basis under paragraph 1(d). Finally, the drafters questioned whether registration was an appropriate basis for asserting criminal jurisdiction since in many cases there would be no meaningful nexus between the offence committed and the State of registry because a

satellite serves as a mere conduit for a transmission.

235. Paragraph 1, *litterae b* and *c* are based upon a variant of the principle of territoriality. These *litterae* require each Party to establish criminal jurisdiction over offences committed upon ships flying its flag or aircraft registered under its laws. This obligation is already implemented as a general matter in the laws of many States, since such ships and aircraft are frequently considered to be an extension of the territory of the State. This type of jurisdiction is most useful where the ship or aircraft is not located in its territory at the time of the commission of the crime, as a result of which Paragraph 1, *littera a* would not be available as a basis to assert jurisdiction. If the crime is committed on a ship or aircraft that is beyond the territory of the flag Party, there may be no other State that would be able to exercise jurisdiction barring this requirement. In addition, if a crime is committed aboard a ship or aircraft which is merely passing through the waters or airspace of another State, the latter State may face significant practical impediments to the exercise of its jurisdiction, and it is therefore useful for the State of registry to also have jurisdiction.

236. Paragraph 1, *littera d* is based upon the principle of nationality. The nationality theory is most frequently applied by States applying the civil law tradition. It provides that nationals of a State are obliged to comply with the domestic law even when they are outside its territory. Under *littera d*, if a national commits an offence abroad, the Party is obliged to have the ability to prosecute it if the conduct is also an offence under the law of the State in which it was committed or the conduct has taken place outside the territorial jurisdiction of any State.

237. Paragraph 2 allows Parties to enter a reservation to the jurisdiction grounds laid down in paragraph 1, *litterae b, c*, and *d*. However, no reservation is permitted with respect to the establishment of territorial jurisdiction under *littera a*, or with respect to the obligation to establish jurisdiction in cases falling under the principle of *"aut dedere aut judicare"* (extradite or prosecute) under paragraph 3, i.e. where that Party has refused to extradite the alleged offender on the basis of his nationality and the offender is present on its territory. Jurisdiction established on the basis of paragraph 3 is necessary to ensure that those Parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if sought by the Party that requested extradition pursuant to the requirements of "Extradition", Article 24, paragraph 6 of this Convention.

238. The bases of jurisdiction set forth in paragraph 1 are not the exclusive. Paragraph 4 of this Article permits the Parties to establish, in conformity with their domestic law, other types of criminal jurisdiction as well.

239. In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in many States. In order to avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings, the affected Parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph. Finally, the obligation to consult is not absolute, but is to take place "where appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation

or proceeding, it may delay or decline consultation.

Chapter III - International co-operation

240. Chapter III contains a number of provisions relating to extradition and mutual legal assistance among the Parties.

Section 1 - General principles

Title 1 – General principles relating to international co-operation

General principles relating to international co-operation (Article 23)

241. Article 23 sets forth three general principles with respect to international co-operation under Chapter III.

242. Initially, the article makes clear that international co-operation is to be provided among Parties "to the widest extent possible." This principle requires Parties to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally.

243. Second, the general scope of the obligation to co-operate is set forth in Article 23: co-operation is to be extended to all criminal offences related to computer systems and data (i.e. the offences covered by Article 14, paragraph 2, *litterae a-b)*, as well as to the collection of evidence in electronic form of a criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of Chapter III are applicable. However, it should be noted that Articles 24 (Extradition), 33 (Mutual assistance regarding the real time collection of traffic data) and 34 (Mutual assistance regarding the interception of content data) permit the Parties to provide for a different scope of application of these measures.

244. Finally, co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws." The latter clause establishes the general principle that the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements as between the parties thereto (described in greater detail in the discussion of Article 27 below), or relevant provisions of domestic law pertaining to international co-operation. This basic principle is explicitly reinforced in Articles 24 (Extradition), 25 (General principles relating to mutual assistance), 26 (Spontaneous information), 27 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements), 28 (Confidentiality and limitation on use), 31 (Mutual assistance regarding accessing of stored computer data), 33 (Mutual assistance regarding the real-time collection of traffic data) and 34 (Mutual assistance regarding the interception of content data).

Title 2 – Principles relating to extradition

Extradition (Article 24)

245. Paragraph 1 specifies that the obligation to extradite applies only to offences established in

accordance with Articles 2-11 of the Convention that 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. The drafters decided to insert a threshold penalty because, under the Convention, Parties may punish some of the offences with a relatively short maximum period of incarceration (e.g., Article 2 - illegal access - and Article 4 - data interference). Given this, the drafters did not believe it appropriate to require that each of the offences established in Articles 2-11 be considered per se extraditable. Accordingly, agreement was reached on a general requirement that an offence is to be considered extraditable if - as in Article 2 of the European Convention on Extradition (ETS N° 24) - the maximum punishment that could be imposed for the offence for which extradition was sought was at least one year's imprisonment. The determination of whether an offence is extraditable does not hinge on the actual penalty imposed in the particular case at hand, but instead on the maximum period that may legally be imposed for a violation of the offence for which extradition is sought.

246. At the same time, in accordance with the general principle that international co-operation under Chapter III should be carried out pursuant to instruments in force between the Parties, Paragraph 1 also provides that where a treaty on extradition or an arrangement on the basis of uniform or reciprocal legislation is in force between two or more Parties (see description of this term in discussion of Article 27 below) which provides for a different threshold for extradition, the threshold provided for in such treaty or arrangement shall apply. For example, many extradition treaties between European countries and non-European countries provide that an offence is extraditable only if the maximum punishment is greater than one year's imprisonment or there is a more severe penalty. In such cases, international extradition practitioners will continue to apply the normal threshold under their treaty practice in order to determine whether an offence is extraditable. Even under the European Convention on Extradition (ETS N° 24), reservations may specify a different minimum penalty for extradition. Among Parties to that Convention, when extradition is sought from a Party that has entered such a reservation, the penalty provided for in the reservation shall be applied in determining whether the offence is extraditable.

247. Paragraph 2 provides that the offences described in paragraph 1 are to be deemed extraditable offences in any extradition treaty between or among the Parties, and are to be included in future treaties they may negotiate among themselves. This does not mean that extradition must be granted on every occasion on which a request is made but rather that the possibility of granting extradition of persons for such offences must be available. Under paragraph 5, Parties are able to provide for other requirements for extradition.

248. Under paragraph 3, a Party that would not grant extradition, either because it has no extradition treaty with the requesting Party or because the existing treaties would not cover a request made in respect of the offences established in accordance with this Convention, may use the Convention itself as a basis for surrendering the person requested, although it is not obligated to do so.

249. Where a Party, instead of relying on extradition treaties, utilises a general statutory scheme to carry out extradition, paragraph 4 requires it to include the offences described in Paragraph 1 among those for which extradition is available.

250. Paragraph 5 provides that the requested Party need not extradite if it is not satisfied that all of the terms and conditions provided for by the applicable treaty or law have been fulfilled. It is thus another example of the principle that co-operation shall be carried out pursuant to the terms of applicable international instruments in force between the Parties, reciprocal arrangements, or

domestic law. For example, conditions and restrictions set forth in the European Convention on Extradition (ETS N° 24) and its Additional Protocols (ETS N°s 86 and 98) will apply to Parties to those agreements, and extradition may be refused on such bases (e.g., Article 3 of the European Convention on Extradition provides that extradition shall be refused if the offence is considered political in nature, or if the request is considered to have been made for the purpose of prosecuting or punishing a person on account of, *inter alia*, race, religion, nationality or political opinion).

251. Paragraph 6 applies the principle "*aut dedere aut judicare*" (extradite or prosecute). Since many States refuse extradition of their nationals, offenders who are found in the Party of which they are a national may avoid responsibility for a crime committed in another Party unless local authorities are obliged to take action. Under paragraph 6, if another Party has sought extradition of the offender, and extradition has been refused on the grounds that the offender is a national of the requested Party, the requested Party must, upon request of the requesting Party, submit the case to its authorities for the purpose of prosecution. If the Party whose extradition request has been refused does not request submission of the case for local investigation and prosecution, there is no obligation on the requested Party to take action. Moreover, if no extradition request has been made, or if extradition has been denied on grounds other than nationality, this paragraph establishes no obligation on the requested Party to submit the case for domestic prosecution. In addition, paragraph 6 requires the local investigation and prosecution to be carried out with diligence; it must be treated as seriously "as in the case of any other offence of a comparable nature" in the Party submitting the case. That Party shall report the outcome of its investigation and proceedings to the Party that had made the request.

252. In order that each Party know to whom its requests for provisional arrest or extradition should be directed, paragraph 7 requires Parties to communicate to the Secretary General of the Council of Europe the name and address of its authorities responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. This provision has been limited to situations in which there is no extradition treaty in force between the Parties concerned because if a bilateral or multilateral extradition treaty is in force between the Parties (such as ETS N° 24), the Parties will know to whom extradition and provisional arrest requests are to be directed without the necessity of a registration requirement. The communication to the Secretary General must be made at the time of signature or when depositing the Party's instrument of ratification, acceptance, approval or accession. It should be noted that designation of an authority does not exclude the possibility of using the diplomatic channel.

Title 3 – General principles relating to mutual assistance

General principles relating to mutual assistance (Article 25)

253. The general principles governing the obligation to provide mutual assistance are set forth in paragraph 1. Co-operation is to be provided "to the widest extent possible." Thus, as in Article 23 ("General principals relating to international co-operation"), mutual assistance is in principle to be extensive, and impediments thereto strictly limited. Second, as in Article 23, the obligation to co-operate applies in principle to both criminal offences related to computer systems and data (i.e. the offences covered by Article 14, paragraph 2, *litterae a-b)*, and to the collection of evidence in electronic form of a criminal offence. It was agreed to impose an obligation to co-operate as to this broad class of crimes because there is the same need for streamlined mechanisms of international co-operation as to both of these categories. However, Articles 34 and 35 permit the Parties to provide for a different scope of application of these measures.

254. Other provisions of this Chapter will clarify that the obligation to provide mutual assistance

is generally to be carried out pursuant to the terms of applicable mutual legal assistance treaties, laws and arrangements. Under paragraph 2, each Party is required to have a legal basis to carry out the specific forms of co-operation described in the remainder of the Chapter, if its treaties, laws and arrangements do not already contain such provisions. The availability of such mechanisms, particularly those in Articles 29 through 35 (Specific provisions – Titles 1, 2, 3), is vital for effective co-operation in computer related criminal matters.

255. Some Parties will not require any implementing legislation in order to apply the provisions referred to in paragraph 2, since provisions of international treaties that establish detailed mutual assistance regimes are considered to be self-executing in nature. It is expected that Parties will either be able to treat these provisions as self executing, already have sufficient flexibility under existing mutual assistance legislation to carry out the mutual assistance measures established under this Chapter, or will be able to rapidly enact any legislation required to do so.

256. Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to. Paragraph 3 does so by (1) empowering the Parties to make urgent requests for co-operation through expedited means of communications, rather than through traditional, much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems; and (2) requiring the requested Party to use expedited means to respond to requests in such circumstances. Each Party is required to have the ability to apply this measure if its mutual assistance treaties, laws or arrangement do not already so provide. The listing of fax and e-mail is indicative in nature; any other expedited means of communication may be used as would be appropriate in the particular circumstances at hand. As technology advances, further expedited means of communicating will be developed that may be used to request mutual assistance. With respect to the authenticity and security requirement contained in the paragraph, the Parties may decide among themselves how to ensure the authenticity of the communications and whether there is a need for special security protections (including encryption) that may be necessary in a particularly sensitive case. Finally, the paragraph also permits the requested Party to require a formal confirmation sent through traditional channels to follow the expedited transmission, if it so chooses.

257. Paragraph 4 sets forth the principle that mutual assistance is subject to the terms of applicable mutual assistance treaties (MLATs) and domestic laws. These regimes provide safeguards for the rights of persons located in the requested Party that may become the subject of a request for mutual assistance. For example, an intrusive measure, such as search and seizure, is not executed on behalf of a requesting Party, unless the requested Party's fundamental requirements for such measure applicable in a domestic case have been satisfied. Parties also may ensure protection of rights of persons in relation to the items seized and provided through mutual legal assistance.

258. However, paragraph 4 does not apply if "otherwise specifically provided in this Chapter." This clause is designed to signal that the Convention contains several significant exceptions to the general principle. The first such exception has been seen in paragraph 2 of this Article, which obliges each Party to provide for the forms of co-operation set forth in the remaining articles of the Chapter (such as preservation, real time collection of data, search and seizure, and

maintenance of a 24/7 network), regardless of whether or not its MLATs, equivalent arrangements or mutual assistance laws currently provide for such measures. Another exception is found in Article 27 which is always to be applied to the execution of requests in lieu of the requested Party's domestic law governing international co-operation in the absence of an MLAT or equivalent arrangement between the requesting and requested Parties. Article 27 provides a system of conditions and grounds for refusal. Another exception, specifically provided for in this paragraph, is that co-operation may not be denied, at least as far as the offences established in Articles 2 – 11 of the Convention are concerned, on the grounds that the requested Party considers the request to involve a "fiscal" offence. Finally, Article 29 is an exception in that it provides that preservation may not be denied on dual criminality grounds, although the possibility of a reservation is provided for in this respect.

259. Paragraph 5 is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance (for example, where a requested Party has reserved its right to require dual criminality with respect to the preservation of data under Article 29, paragraph 4 "Expedited preservation of stored computer data"), dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in denominating the offence. This provision was believed necessary in order to ensure that requested Parties do not adopt too rigid a test when applying dual criminality. Given differences in national legal systems, variations in terminology and categorisation of criminal conduct are bound to arise. If the conduct constitutes a criminal violation under both systems, such technical differences should not impede assistance. Rather, in matters in which the dual criminality standard is applicable, it should be applied in a flexible manner that will facilitate the granting of assistance.

Spontaneous information (Article 26)

260. This article is derived from provisions in earlier Council of Europe instruments, such as Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS N° 141) and Article 28 of the Criminal Law Convention on Corruption (ETS N° 173). More and more frequently, a Party possesses valuable information that it believes may assist another Party in a criminal investigation or proceeding, and which the Party conducting the investigation or proceeding is not aware exists. In such cases, no request for mutual assistance will be forthcoming. Paragraph 1 empowers the State in possession of the information to forward it to the other State without a prior request. The provision was thought useful because, under the laws of some States, such a positive grant of legal authority is needed in order to provide assistance in the absence of a request. A Party is not obligated to spontaneously forward information to another Party; it may exercise its discretion in light of the circumstances of the case at hand. Moreover, the spontaneous disclosure of information does not preclude the disclosing Party, if it has jurisdiction, from investigating or instituting proceedings in relation to the facts disclosed.

261. Paragraph 2 addresses the fact that in some circumstances, a Party will only forward information spontaneously if sensitive information will be kept confidential or other conditions can be imposed on the use of information. In particular, confidentiality will be an important consideration in cases in which important interests of the providing State may be endangered should the information be made public, e.g., where there is a need to protect the identity of a means of collecting the information or the fact that a criminal group is being investigated. If advance inquiry reveals that the receiving Party cannot comply with a condition sought by the providing Party (for example, where it cannot comply with a condition of confidentiality because

the information is needed as evidence at a public trial), the receiving Party shall advise the providing Party, which then has the option of not providing the information. If the receiving Party agrees to the condition, however, it must honour it. It is foreseen that conditions imposed under this article would be consistent with those that could be imposed by the providing Party pursuant to a request for mutual assistance from the receiving Party.

Title 4 - Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Procedures pertaining to mutual assistance requests in the absence of applicable international agreements (Article 27)

262. Article 27 obliges the Parties to apply certain mutual assistance procedures and conditions 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 Article thus reinforces the general principle that mutual assistance should be carried out through application of relevant treaties and similar arrangements for mutual assistance. The drafters rejected the creation of a separate general regime of mutual assistance in this Convention that would be applied in lieu of other applicable instruments and arrangements, agreeing instead that it would be more practical to rely on existing MLAT regimes as a general matter, thereby permitting mutual assistance practitioners to use the instruments and arrangements they are the most familiar with and avoiding confusion that may result from the establishment of competing regimes. As previously stated, only with respect to mechanisms particularly necessary for rapid effective co-operation in computer related criminal matters, such as those in Articles 29-35 (Specific provisions – Title 1, 2, 3), is each Party required to establish a legal basis to enable the carrying out of such forms of co-operation if its current mutual assistance treaties, arrangements or laws do not already do so.

263. Accordingly, most forms of mutual assistance under this Chapter will continue to be carried out pursuant to the European Convention on Mutual Assistance in Criminal Matters (ETS N° 30) and its Protocol (ETS N° 99) among the Parties to those instruments. Alternatively, Parties to this Convention that have bilateral MLATs in force between them, or other multilateral agreements governing mutual assistance in criminal cases (such as between member States of the European Union), shall continue to apply their terms, supplemented by the computer- or computer-related crime-specific mechanisms described in the remainder of Chapter III, unless they agree to apply any or all of the provisions of this Article in lieu thereof. Mutual assistance may also be based on arrangements agreed on the basis of uniform or reciprocal legislation, such as the system of co-operation developed among the Nordic countries, which is also admitted by the European Convention on Mutual Assistance in Criminal Matters (Article 25, paragraph 4), and among members of the Commonwealth. Finally, the reference to mutual assistance treaties or arrangements on the basis of uniform or reciprocal legislation is not limited to those instruments in force at the time of entry into force of the present Convention, but also covers instruments that may be adopted in the future.

264. Article 27 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements), paragraphs 2-10, provide a number of rules for providing mutual assistance in the absence of an MLAT or arrangement on the basis of uniform or reciprocal legislation, including establishment of central authorities, imposing of conditions, grounds for and procedures in cases of postponement or refusal, confidentiality of requests, and direct communications. With respect to such expressly covered issues, in the absence of a mutual assistance agreement or arrangement on the basis of uniform or reciprocal legislation, the provisions of this Article are to be applied in lieu of otherwise applicable domestic laws governing

mutual assistance. At the same time, Article 27 does not provide rules for other issues typically dealt with in domestic legislation governing international mutual assistance. For example, there are no provisions dealing with the form and contents of requests, taking of witness testimony in the requested or requesting Parties, the providing of official or business records, transfer of witnesses in custody, or assistance in confiscation matters. With respect to such issues, Article 25, paragraph 4 provides that absent a specific provision in this Chapter, the law of the requested Party shall govern specific modalities of providing that type of assistance.

265. Paragraph 2 requires the establishment of a central authority or authorities responsible for sending and answering requests for assistance. The institution of central authorities is a common feature of modern instruments dealing with mutual assistance in criminal matters, and it is particularly helpful in ensuring the kind of rapid reaction that is so useful in combating computer- or computer-related crime. Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly.

266. Parties are encouraged as a matter of efficiency to designate a single central authority for the purpose of mutual assistance; it would generally be most efficient for the authority designated for such purpose under a Party's MLATs, or domestic law to also serve as the central authority when this article is applicable. However, a Party has the flexibility to designate more than one central authority where this is appropriate under its system of mutual assistance. Where more than one central authority is established, the Party that has done so should ensure that each authority interprets the provisions of the Convention in the same way, and that both incoming and outgoing requests are treated rapidly and efficiently. Each Party is to advise the Secretary General of the Council of Europe of the names and addresses (including e-mail and fax numbers) of the authority or authorities designated to receive and respond to mutual assistance requests under this Article, and Parties are obliged to ensure that the designation is kept up-to-date.

267. A major objective of a State requesting mutual assistance often is to ensure that its domestic laws governing the admissibility of evidence are fulfilled, and it can use the evidence before its courts as a result. To ensure that such evidentiary requirements can be met, paragraph 3 obliges the requested Party to execute requests in accordance with the procedures specified by the requesting Party, unless to do so would be incompatible with its law. It is emphasised that this paragraph relates only to the obligation to respect technical procedural requirements, not to fundamental procedural protections. Thus, for example, a requesting Party cannot require the requested Party to execute a search and seizure that would not meet the requested Party's fundamental legal requirements for this measure. In light of the limited nature of the obligation, it was agreed 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; instead, the procedure must be incompatible with the requested Party's legal principles. For example, under the law of the requesting Party, it may be a procedural requirement that a statement of a witness be given under oath. Even if the requested Party does not domestically have the requirement that statements be given under oath, it should honour the requesting Party's request.

268. Paragraph 4 provides for the possibility of refusing requests for mutual assistance requests brought under this Article. Assistance may be refused on the grounds provided for in Article 25, paragraph 4 (i.e. grounds provided for in the law of the requested Party), including prejudice to the sovereignty of the State, security, *ordre public* or other essential interests, and where the

offence is considered by the requested Party to be a political offence or an offence connected with a political offence. In order to promote the overriding principle of providing the widest measure of co-operation (see Articles 23, 25), grounds for refusal established by a requested Party should be narrow and exercised with restraint. They may not be so expansive as to create the potential for assistance to be categorically denied, or subjected to onerous conditions, with respect to broad categories of evidence or information.

269. In line with this approach, it was understood that apart from those grounds set out in Article 28, refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal. A broad, categorical, or systematic application of data protection principles to refuse cooperation is therefore precluded. Thus, the fact the Parties concerned have different systems of protecting the privacy of data (such as that the requesting Party does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting Party uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), do not as such constitute grounds for refusal. Before invoking "essential interests" as a basis for refusing co-operation, the requested Party should instead attempt to place conditions which would allow the transfer of the data. (see Article 27, paragraph 6 and paragraph 271 of this report).

270. Paragraphs 5 permits the requested Party to postpone, rather than refuse, assistance where immediate action on the request would be prejudicial to investigations or proceedings in the requested Party. For example, where the requesting Party has sought to obtain evidence or witness testimony for purposes of investigation or trial, and the same evidence or witness are needed for use at a trial that is about to commence in the requested Party, the requested Party would be justified in postponing the providing of assistance.

271. Paragraph 6 provides that where the assistance sought would otherwise be refused or postponed, the requested Party may instead provide assistance subject to conditions. If the conditions are not agreeable to the requesting Party, the requested Party may modify them, or it may exercise its right to refuse or postpone assistance. Since the requested Party has an obligation to provide the widest possible measure of assistance, it was agreed that both grounds for refusal and conditions should be exercised with restraint.

272. Paragraph 7 obliges the requested Party to keep the requesting Party informed of the outcome of the request, and requires reasons to be given in the case of refusal or postponement of assistance. The providing of reasons can, *inter alia*, assist the requesting Party to understand how the requested Party interprets the requirements of this Article, provide a basis for consultation in order to improve the future efficiency of mutual assistance, and provide to the requesting Party previously unknown factual information about the availability or condition of witnesses or evidence.

273. There are times when a Party makes a request in a particularly sensitive case, or in a case in which there could be disastrous consequences if the facts underlying the request were to be made public prematurely. Paragraph 8 accordingly permits the requesting Party to request that the fact and content of the request be kept confidential. Confidentiality may not be sought, however, to the extent that it would undermine the requested Party's ability to obtain the evidence or information

possession of the data from its custodian. The preferred procedure is for the requested Party to ensure that the custodian (frequently a service provider or other third party) preserve (i.e., not delete) the data pending the issuance of process requiring it to be turned over to law enforcement officials at a later stage. This procedure has the advantage of being both rapid and protective of the privacy of the person whom the data concerns, as it will not be disclosed to or examined by any government official until the criteria for full disclosure pursuant to normal mutual assistance regimes have been fulfilled. At the same time, a requested Party is permitted to use other procedures for ensuring the rapid preservation of data, including the expedited issuance and execution of a production order or search warrant for the data. The key requirement is to have an extremely rapid process in place to prevent the data from being irretrievably lost.

284. Paragraph 2 sets forth the contents of a request for preservation pursuant to this Article. Bearing in mind that this is a provisional measure and that a request will need to be prepared and transmitted rapidly, the information provided will be summary and include only the minimum information required to enable preservation of the data. In addition to specifying the authority that is seeking preservation and the offence for which the measure is sought, the request must provide a summary of the facts, information sufficient to identify the data to be preserved and its location, and a showing that the data is relevant to the investigation or prosecution of the offence concerned and that preservation is necessary. Finally, the requesting Party must undertake to subsequently submit a request for mutual assistance so that it may obtain production of the data.

285. Paragraph 3 sets forth the principle that dual criminality shall not be required as a condition to providing preservation. In general, application of the principle of dual criminality is ~~counterproductive in the context of preservation. First, as a matter of modern mutual assistance~~ practice, there is a trend to eliminate the dual criminality requirement for all but the most intrusive procedural measures, such as search and seizure or interception. Preservation as foreseen by the drafters, however, is not particularly intrusive, since the custodian merely maintains possession of data lawfully in its possession, and the data is not disclosed to or examined by officials of the requested Party until after execution of a formal mutual assistance request seeking disclosure of the data. Second, as a practical matter, it often takes so long to provide the clarifications necessary to conclusively establish the existence of dual criminality that the data would be deleted, removed or altered in the meantime. For example, at the early stages of an investigation, the requesting Party may be aware that there has been an intrusion into a computer in its territory, but may not until later have a good understanding of the nature and extent of damage. If the requested Party were to delay preserving traffic data that would trace the source of the intrusion pending conclusive establishment of dual criminality, the critical data would often be routinely deleted by service providers holding it for only hours or days after the transmission has been made. Even if thereafter the requesting Party were able to establish dual criminality, the crucial traffic data could not be recovered and the perpetrator of the crime would never be identified.

286. Accordingly, the general rule is that Parties must dispense with any dual criminality requirement for the purpose of preservation. However, a limited reservation is available under paragraph 4. If a Party requires dual criminality as a condition for responding to a request for mutual assistance for production of the data, and if it has reason to believe that, at the time of disclosure, dual criminality will not be satisfied, it may reserve the right to require dual criminality as a precondition to preservation. With respect to offences established in accordance with Articles 2 through 11, it is assumed that the condition of dual criminality is automatically met between the Parties, subject to any reservations they may have entered to these offences where permitted by the Convention. Therefore, Parties may impose this requirement only in relation to offences other than those defined in the Convention.

287. Otherwise, under paragraph 5, the requested Party may only refuse a request for preservation where its execution will prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. Due to the centrality of this measure to the effective investigation and prosecution of computer- or computer-related crime, it was agreed that the assertion of any other basis for refusing a request for preservation is precluded.

288. At times, the requested Party will realise that the custodian of the data is likely to take action that will threaten the confidentiality of, or otherwise prejudice, the requesting Party's investigation (for example, where the data to be preserved is held by a service provider controlled by a criminal group, or by the target of the investigation himself). In such situations, under paragraph 6, the requesting Party must be notified promptly, so that it may assess whether to take the risk posed by carrying through with the request for preservation, or to seek a more intrusive but safer form of mutual assistance, such as production or search and seizure.

289. Finally, paragraph 7 obliges each Party to ensure that data preserved pursuant to this Article will be held for at least 60 days pending receipt of a formal mutual assistance request seeking the disclosure of the data, and continue to be held following receipt of the request.

Expedited disclosure of preserved traffic data (Article 30)

290. This article provides the international equivalent of the power established for domestic use in Article 17. Frequently, at the request of a Party in which a crime was committed, a requested Party will preserve traffic data regarding a transmission that has travelled through its computers, in order to trace the transmission to its source and identify the perpetrator of the crime, or locate critical evidence. In doing so, the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself. In such cases, the requested Party must expeditiously provide to the requesting Party a sufficient amount of the traffic data to enable identification of the service provider in, and path of the communication from, the other State. If the transmission came from a third State, this information will enable the requesting Party to make a request for preservation and expedited mutual assistance to that other State in order to trace the transmission to its ultimate source. If the transmission had looped back to the requesting Party, it will be able to obtain preservation and disclosure of further traffic data through domestic processes.

291. Under Paragraph 2, the requested Party may only refuse to disclose the traffic data, where disclosure is likely to prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. As in Article 29 (Expedited preservation of stored computer data), because this type of information is so crucial to identification of those who have committed crimes within the scope of this Convention or locating of critical evidence, grounds for refusal are to be strictly limited, and it was agreed that the assertion of any other basis for refusing assistance is precluded.

Title 2 - Mutual assistance regarding investigative powers

Mutual assistance regarding accessing of stored computer data (Article 31)

292. Each Party must have the ability to, for the benefit of another Party, search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within its territory - just as under Article 19 (Search and seizure of stored computer data) it must

have the ability to do so for domestic purposes. Paragraph 1 authorises a Party to request this type of mutual assistance, and paragraph 2 requires the requested Party to be able to provide it. Paragraph 2 also follows the principle that the terms and conditions for providing such co-operation should be those set forth in applicable treaties, arrangements and domestic laws governing mutual legal assistance in criminal matters. Under paragraph 3, such a request must be responded to on an expedited basis where (1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or (2) otherwise where such treaties, arrangements or laws so provide.

Transborder access to stored computer data with consent or where publicly available (Article 32)

293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.

294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

Mutual assistance regarding the real-time collection of traffic data (Article 33)

295. In many cases, investigators cannot ensure that they are able to trace a communication to its source by following the trail through records of prior transmissions, as key traffic data may have been automatically deleted by a service provider in the chain of transmission before it could be preserved. It is therefore critical for investigators in each Party to have the ability to obtain traffic data in real time regarding communications passing through a computer system in other Parties. Accordingly, under Article 33 (Mutual assistance regarding the real-time collection of traffic data), each Party is under the obligation to collect traffic data in real time for another Party. While this Article requires the Parties to co-operate on these matters, here, as elsewhere, deference is given to existing modalities of mutual assistance. Thus, the terms and conditions by which such co-operation is to be provided are generally those set forth in applicable treaties, arrangements and laws governing mutual legal assistance in criminal matters.

296. In many countries, mutual assistance is provided broadly with respect to the real time collection of traffic data, because such collection is viewed as being less intrusive than either interception of content data, or search and seizure. However, a number of States take a narrower approach. Accordingly, in the same way as the Parties may enter a reservation under Article 14 (Scope of procedural provisions), paragraph 3, with respect to the scope of the equivalent domestic measure, paragraph 2 permits Parties to limit the scope of application of this measure to a more narrow range of offences than provided for in Article 23 (General principles relating to international co-operation). One caveat is provided: in no event may the range of offences be more narrow than the range of offences for which such measure is available in an equivalent domestic case. Indeed, because real time collection of traffic data is at times the only way of ascertaining the identity of the perpetrator of a crime, and because of the lesser intrusiveness of the measure, the use of the term "at least" in paragraph 2 is designed to encourage Parties to permit as broad assistance as possible, i.e., even in the absence of dual criminality.

Mutual assistance regarding the interception of content data (Article 34)

297. Because of the high degree of intrusiveness of interception, the obligation to provide mutual assistance for interception of content data is restricted. The assistance is to be provided to the extent permitted by the Parties' applicable treaties and laws. As the provision of co-operation for interception of content is an emerging area of mutual assistance practice, it was decided to defer to existing mutual assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist. In this regard, reference is made to the comments on Articles 14, 15 and 21 as well as to 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.

Title 3 - 24/7 Network

24/7 Network (Article 35)

298. As has been previously discussed, effective combating of crimes committed by use of computer systems and effective collection of evidence in electronic form requires very rapid response. Moreover, with a few keystrokes, action may be taken in one part of the world that instantly has consequences many thousands of kilometres and many time zones away. For this reason, existing police co-operation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively. The channel established in this Article is based upon the experience gained from an already functioning network created under the auspices of the G8 group of nations. Under this Article, each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings within the scope of this Chapter, in particular as defined under Article 35, paragraph 1, *litterae a) – c)*. It was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer- or computer-related crime.

299. Each Party's 24/7 point of contact is to either facilitate or directly carry out, *inter alia*, the providing of technical advice, preservation of data, collection of evidence, giving of legal information, and locating of suspects. The term "legal information" in Paragraph 1 means advice to another Party that is seeking co-operation of any legal prerequisites required for providing informal or formal co-operation.

300. Each Party is at liberty to determine where to locate the point of contact within its law enforcement structure. Some Parties may wish to house the 24/7 contact within its central authority for mutual assistance, some may believe that the best location is with a police unit specialised in fighting computer- or computer-related crime, yet other choices may be appropriate for a particular Party, given its governmental structure and legal system. Since the 24/7 contact is to provide both technical advice for stopping or tracing an attack, as well as such international co-operation duties as locating of suspects, there is no one correct answer, and it is anticipated that the structure of the network will evolve over time. In designating the national point of contact, due consideration should be given to the need to communicate with points of contacts using other languages.

301. Paragraph 2 provides that among the critical tasks to be carried out by the 24/7 contact is the ability to facilitate the rapid execution of those functions it does not carry out directly itself. For example, if a Party's 24/7 contact is part of a police unit, it must have the ability to co-ordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance, in order that appropriate action may be taken at any hour of the day or night. Moreover, paragraph 2 requires each Party's 24/7 contact to have the capacity to carry out communications with other members of the network on an expedited basis.

302. Paragraph 3 requires each point of contact in the network to have proper equipment. Up-to-date telephone, fax and computer equipment will be essential to the smooth operation of the network, and other forms of communication and analytical equipment will need to be part of the system as technology advances. Paragraph 3 also requires that personnel participating as part of a ~~Party's team for the network be properly trained regarding computer- or computer-related crime~~ and how to respond to it effectively.

Chapter IV – Final provisions

303. With some exceptions, the provisions contained in this Chapter are, for the most part, based on the 'Model final clauses for conventions and agreements concluded within the Council of Europe' which were approved by the Committee of Ministers at the 315th meeting of the Deputies in February 1980. As most of the articles 36 through 48 either use the standard language of the model clauses or are based on long-standing treaty-making practice at the Council of Europe, they do not call for specific comments. However, certain modifications of the standard model clauses or some new provisions require some explanation. It is noted in this context that the model clauses have been adopted as a non-binding set of provisions. As the Introduction to the Model Clauses pointed out "these model final clauses are only intended to facilitate the task of committees of experts and avoid textual divergences which would not have any real justification. The model is in no way binding and different clauses may be adapted to fit particular cases."

Signature and entry into force (Article 36)

304. Article 36, paragraph 1, has been drafted following several precedents established in other conventions elaborated within the framework of the Council of Europe, for instance, the Convention on the Transfer of Sentenced Persons (ETS No. 112) and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141), which allow for signature, before their entry into force, not only by the member States of the Council of Europe, but also by non-member States which have participated in their elaboration. The provision is intended to enable the maximum number of interested States, not just members of the Council of Europe, to become Parties as soon as possible. Here, the provision is intended to apply to four non-member States, Canada, Japan, South Africa and the United States of America, which

actively participated in the elaboration of the Convention. Once the Convention enters into force, in accordance with paragraph 3, other non-member States not covered by this provision may be invited to accede to the Convention in conformity with Article 37, paragraph 1.

305. Article 36, paragraph 3 sets the number of ratifications, acceptances or approvals required for the Convention's entry into force at 5. This figure is higher than the usual threshold (3) in Council of Europe treaties and reflects the belief that a slightly larger group of States is needed to successfully begin addressing the challenge of international computer- or computer-related crime. The number is not so high, however, so as not to delay unnecessarily the Convention's entry into force. Among the five initial States, at least three must be Council of Europe members, but the two others could come from the four non-member States that participated in the Convention's elaboration. This provision would of course also allow for the Convention to enter into force based on expressions of consent to be bound by five Council of Europe member States.

Accession to the Convention (Article 37)

306. Article 37 has also been drafted on precedents established in other Council of Europe conventions, but with an additional express element. Under long-standing practice, the Committee of Ministers decides, on its own initiative or upon request, to invite a non-member State, which has not participated in the elaboration of a convention, to accede to the convention after having consulted all contracting Parties, whether member States or not. This implies that if any contracting Party objects to the non-member State's accession, the Committee of Ministers would usually not invite it to join the convention. However, under the usual formulation, the Committee of Ministers could - in theory - invite such a non-member State to accede to a convention even if a non-member State Party objected to its accession. This means that - in theory - no right of veto is usually granted to non-member States Parties in the process of extending Council of Europe treaties to other non-member States. However, an express requirement that the Committee of Ministers consult with and obtain the unanimous consent of all Contracting States – not just members of the Council of Europe – before inviting a non-member State to accede to the Convention has been inserted. As indicated above, such a requirement is consistent with practice and recognises that all Contracting States to the Convention should be able to determine with which non-member States they are to enter into treaty relations. Nevertheless, the formal decision to invite a non-member State to accede will be taken, in accordance with usual practice, by the representatives of the contracting Parties entitled to sit on the Committee of Ministers. This decision requires the two-thirds majority provided for in Article 20.d of the Statute of the Council of Europe and the unanimous vote of the representatives of the contracting Parties entitled to sit on the Committee.

307. Federal States seeking to accede to the Convention, which intend to make a declaration under Article 41, are required to submit in advance a draft of the statement referred to in Article 41, paragraph 3, so that the Parties will be in a position to evaluate how the application of the federal clause would affect the prospective Party's implementation of the Convention.(see paragraph 320).

Effects of the Convention (Article 39)

308. Article 39, paragraphs 1 and 2 address the Convention's relationship to other international agreements or arrangements. The subject of how conventions of the Council of Europe should relate to one another or to other treaties, bilateral or multilateral, concluded outside the Council of Europe is not dealt with by the Model Clauses referred to above. The usual approach utilised in Council of Europe conventions in the criminal law area (e.g., Agreement on Illicit Traffic by Sea

(ETS N° 156)) is to provide that: (1) new conventions do not affect the rights and undertakings derived from existing international multilateral conventions concerning special matters; (2) Parties to a new convention may conclude bilateral or multilateral agreements with one another on the matters dealt with by the convention for the purposes of supplementing or strengthening its provisions or facilitating the application of the principles embodied in it; and (3) if two or more Parties to the new convention have already concluded an agreement or treaty in respect of a subject which is dealt with in the convention or otherwise have established their relations in respect of that subject, they shall be entitled to apply that agreement or treaty or to regulate those relations accordingly, in lieu of the new convention, provided this facilitates international co-operation.

309. Inasmuch as the Convention generally is intended to supplement and not supplant multilateral and bilateral agreements and arrangements between Parties, the drafters did not believe that a possibly limiting reference to "special matters" was particularly instructive and were concerned that it could lead to unnecessary confusion. Instead, paragraph 1 of Article 39 simply indicates that the present Convention supplements other applicable treaties or arrangements as between Parties and it mentions in particular three Council of Europe treaties as non-exhaustive examples: the 1957 European Convention on Extradition (ETS N° 24), the 1959 European Convention on Criminal Matters (ETS N° 30) and its 1978 Additional Protocol (ETS N° 99). Therefore, regarding general matters, such agreements or arrangements should in principle be applied by the Parties to the Convention on cybercrime. Regarding specific matters only dealt with by this Convention, the rule of interpretation *lex specialis derogat legi generali* provides that the Parties should give precedence to the rules contained in the Convention. An example is Article 30, which provides for the expedited disclosure of preserved traffic data when necessary to identify the path of a specified communication. In this specific area, the Convention, as *lex specialis*, should provide a rule of first resort over provisions in more general mutual assistance agreements.

310. Similarly, the drafters considered language making the application of existing or future agreements contingent on whether they "strengthen" or "facilitate" co-operation as possibly problematic, because, under the approach established in the international co-operation Chapter, the presumption is that Parties will apply relevant international agreements and arrangements.

311. Where there is an existing mutual assistance treaty or arrangement as a basis for co-operation, the present Convention would only supplement, where necessary, the existing rules. For example, this Convention would provide for the transmission of mutual assistance requests by expedited means of communications (see Article 25, paragraph 3) if such a possibility does not exist under the original treaty or arrangement.

312. Consistent with the Convention's supplementary nature and, in particular, its approach to international co-operation, paragraph 2 provides that Parties are also free to apply agreements that already are or that may in the future come into force. Precedent for such an articulation is found in the Transfer of Sentenced Persons Convention (ETS N° 112). Certainly, in the context of international co-operation, it is expected that application of other international agreements (many of which offer proven, longstanding formulas for international assistance) will in fact promote co-operation. Consistent with the terms of the present Convention, Parties may also agree to apply its international co-operation provisions in lieu of such other agreements (see Article 27(1)). In such instances the relevant co-operation provisions set forth in Article 27 would supersede the relevant rules in such other agreements. As the present Convention generally provides for minimum obligations, Article 39, paragraph 2 recognises that Parties are free to assume obligations that are more specific in addition to those already set out in the Convention, when establishing their

relations concerning matters dealt with therein. However, this is not an absolute right: Parties must respect the objectives and principles of the Convention when so doing and therefore cannot accept obligations that would defeat its purpose.

313. Further, in determining the Convention's relationship to other international agreements, the drafters also concurred that Parties may look for additional guidance to relevant provisions in the Vienna Convention on the Law of Treaties.

314. While the Convention provides a much-needed level of harmonisation, it does not purport to address all outstanding issues relating to computer- or computer-related crime. Therefore, paragraph 3 was inserted to make plain that the Convention only affects what it addresses. Left unaffected are other rights, restrictions, obligations and responsibilities that may exist but that are not dealt with by the Convention. Precedent for such a "savings clause" may be found in other international agreements (e.g., UN Terrorist Financing Convention).

Declarations (Article 40)

315. Article 40 refers to certain articles, mostly in respect of the offences established by the Convention in the substantive law section, where Parties are permitted to include certain specified additional elements which modify the scope of the provisions. Such additional elements aim at accommodating certain conceptual or legal differences, which in a treaty of global ambition are more justified than they perhaps might be in a purely Council of Europe context. Declarations are considered acceptable interpretations of Convention provisions and should be distinguished from reservations, which permit a Party to exclude or to modify the legal effect of certain obligations set forth in the Convention. Since it is important for Parties to the Convention to know which, if any, additional elements have been attached by other Parties, there is an obligation to declare them to the Secretary General of the Council of Europe at the time of signature or when depositing an instrument of ratification, acceptance, approval or accession. Such notification is particularly important concerning the definition of offences, as the condition of dual criminality will have to be met by the Parties when applying certain procedural powers. No numerical limit was felt necessary in respect of declarations.

Federal clause (Article 41)

316. Consistent with the goal of enabling the largest possible number of States to become Parties, Article 41 allows for a reservation which is intended to accommodate the difficulties federal States may face as a result of their characteristic distribution of power between central and regional authorities. Precedents exist outside the criminal law area for federal declarations or reservations to other international agreements (11). Here, Article 41 recognises that minor variations in coverage may occur as a result of well-established domestic law and practice of a Party which is a federal State. Such variations must be based on its Constitution or other fundamental principles concerning the division of powers in criminal justice matters between the central government and the constituent States or territorial entities of a federal State. There was agreement among the drafters of the Convention that the operation of the federal clause would only lead to minor variations in the application of the Convention.

317. For example, in the United States, under its Constitution and fundamental principles of federalism, federal criminal legislation generally regulates conduct based on its effects on interstate or foreign commerce, while matters of minimal or purely local concern are traditionally regulated by the constituent States. This approach to federalism still provides for broad coverage

of illegal conduct encompassed by this Convention under US federal criminal law, but recognises that the constituent States would continue to regulate conduct that has only minor impact or is purely local in character. In some instances, within that narrow category of conduct regulated by State but not federal law, a constituent State may not provide for a measure that would otherwise fall within the scope of this Convention. For example, an attack on a stand-alone personal computer, or network of computers linked together in a single building, may only be criminal if provided for under the law of the State in which the attack took place; however the attack would be a federal offence if access to the computer took place through the Internet, since the use of the Internet provides the effect on interstate or foreign commerce necessary to invoke federal law. The implementation of this Convention through United States federal law, or through the law of another federal State under similar circumstances, would be in conformity with the requirements of Article 41.

318. The scope of application of the federal clause has been restricted to the provisions of Chapter II (substantive criminal law, procedural law and jurisdiction). Federal States making use of this provision would still be under the obligation to co-operate with the other Parties under Chapter III, even where the constituent State or other similar territorial entity in which a fugitive or evidence is located does not criminalise conduct or does not have procedures required under the Convention.

319. In addition, paragraph 2 of Article 41 provides that a federal State, when making a reservation under paragraph 1 of this Article, may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures. In respect of provisions the implementation of which come within the legislative jurisdiction of the constituent States or other similar territorial entities, the federal government shall refer the provisions to the authorities of these entities with a favourable endorsement, encouraging them to take appropriate action to give them effect. .

Reservations (Article 42)

320. Article 42 provides for a number of reservation possibilities. This approach stems from the fact that the Convention covers an area of criminal law and criminal procedural law which is relatively new to many States. In addition, the global nature of the Convention, which will be open to member and non-member States of the Council of Europe, makes having such reservation possibilities necessary. These reservation possibilities aim at enabling the largest number of States to become Parties to the Convention, while permitting such States to maintain certain approaches and concepts consistent with their domestic law. At the same time, the drafters endeavoured to restrict the possibilities for making reservations in order to secure to the largest possible extent the uniform application of the Convention by the Parties. Thus, no other reservations may be made than those enumerated. In addition, reservations may only be made by a Party at the time of signature or upon deposit of its instrument of ratification, acceptance, approval or accession.

321. Recognising that for some Parties certain reservations were essential to avoid conflict with their constitutional or fundamental legal principles, Article 43 imposes no specific time limit for the withdrawal of reservations. Instead, they should be withdrawn as soon as circumstances so permit.

322. In order to maintain some pressure on the Parties and to make them at least consider withdrawing their reservations, the Convention authorises the Secretary General of the Council of Europe to periodically enquire about the prospects for withdrawal. This possibility of enquiry is current practice under several Council of Europe instruments. The Parties are thus given an

opportunity to indicate whether they still need to maintain their reservations in respect of certain provisions and to withdraw, subsequently, those which no longer prove necessary. It is hoped that over time Parties will be able to remove as many of their reservations as possible so as promote the Convention's uniform implementation.

Amendments (Article 44)

323. Article 44 takes its precedent from the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS N° 141), where it was introduced as an innovation in respect of criminal law conventions elaborated within the framework of the Council of Europe. The amendment procedure is mostly thought to be for relatively minor changes of a procedural and technical character. The drafters considered that major changes to the Convention could be made in the form of additional protocols.

324. The Parties themselves can examine the need for amendments or protocols under the consultation procedure provided for in Article 46. The European Committee on Crime Problems (CDPC) will in this regard be kept periodically informed and required to take the necessary measures to assist the Parties in their efforts to amend or supplement the Convention.

325. In accordance with paragraph 5, any amendment adopted would come into force only when all Parties have informed the Secretary General of their acceptance. This requirement seeks to ensure that the Convention will evolve in a uniform manner.

Settlement of disputes (Article 45)

326. Article 45, paragraph 1, provides that the European Committee on Crime Problems (CDPC) should be kept informed about the interpretation and application of the provisions of the Convention. Paragraph 2 imposes an obligation on the Parties to seek a peaceful settlement of any dispute concerning the interpretation or the application of the Convention. Any procedure for solving disputes should be agreed upon by the Parties concerned. Three possible mechanisms for dispute-resolution are suggested by this provision: the European Committee on Crime Problems (CDPC) itself, an arbitral tribunal or the International Court of Justice.

Consultations of the Parties (Article 46)

327. Article 46 creates a framework for the Parties to consult regarding implementation of the Convention, the effect of significant legal, policy or technological developments pertaining to the subject of computer- or computer-related crime and the collection of evidence in electronic form, and the possibility of supplementing or amending the Convention. The consultations shall in particular examine issues that have arisen in the use and implementation of the Convention, including the effects of declarations and reservations made under Articles 40 and 42.

328. The procedure is flexible and it is left to the Parties to decide how and when to convene if they so wish. Such a procedure was believed necessary by the drafters of the Convention to ensure that all Parties to the Convention, including non-member States of the Council of Europe, could be involved - on an equal footing basis - in any follow-up mechanism, while preserving the competences of the European Committee on Crime Problems (CDPC). The latter shall not only be kept regularly informed of the consultations taking place among the Parties, but also facilitate those and take the necessary measures to assist the Parties in their efforts to supplement or amend the Convention. Given the needs of effective prevention and prosecution of cyber-crime and the

associated privacy issues, the potential impact on business activities, and other relevant factors, the views of interested parties, including law enforcement, non-governmental and private sector organisations, may be useful to these consultations (see also paragraph 14).

329. Paragraph 3 provides for a review of the Convention's operation after 3 years of its entry into force, at which time appropriate amendments may be recommended. The CDPC shall conduct such review with the assistance of the Parties.

330. Paragraph 4 indicates that except where assumed by the Council of Europe it will be for the Parties themselves to finance any consultations carried out in accordance with paragraph 1 of Article 46. However, apart from the European Committee on Crime Problems (CDPC), the Council of Europe Secretariat shall assist the Parties in their efforts under the Convention.

Notes :

(1) 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). Back.

(2) See Computer-related crime, Report by the European Committee on Crime Problems, page 86. Back.

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

(4) The text of the Convention had been amended according to the provisions of Protocol No. 3 (ETS No. 45), which entered into force on 21 September 1970, of Protocol No. 5 (ETS No. 55), which entered into force on 20 December 1971 and of Protocol No. 8 (ETS No. 118), which entered into force on 1 January 1990, and comprised also the text of Protocol No. 2 (ETS No. 44) which, in accordance with Article 5, paragraph 3 thereof, had been an integral part of the Convention since its entry into force on 21 September 1970. All provisions which had been amended or added by these Protocols are replaced by Protocol No. 11 (ETS No. 155), as from the date of its entry into force on 1 November 1998. As from that date, Protocol No. 9 (ETS No. 140), which entered into force on 1 October 1994, is repealed and Protocol No. 10 (ETS No. 146) has lost its purpose. Back.

(5) ECHR Judgment in the case of Klass and others v. Germany, A28, 06/09/1978. Back.

(6) ECHR Judgment in the case of Kruslin v. France, 176-A, 24/04/1990. Back.

(7) ECHR Judgment in the case of Huvig v. France, 176-B, 24/04/1990. Back.

(8) ECHR Judgment in the case of Malone v. United Kingdom, A82, 02/08/1984. Back.

(9) ECHR Judgment in the case of Halford v. United Kingdom, Reports 1997 – III, 25/06/1997. Back.

(10) ECHR Judgment in the case of Lambert v. France, Reports 1998 – V, 24/08/1998. Back.

(11) E.g. Convention Relating to the Status of Refugees of 28 July 1951, Art. 34; Convention Relating to the Status of Stateless Persons of 28 September 1954, Art. 37; Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 10 June 1958, Art. 11; Convention for the Protection of World Cultural and Natural Heritage of 16 November 1972, Art. 34. Back.

O