UNITED NATIONS CONFERENCE
ON TRADE AND DEVELOPMENT

EAST AFRICAN COMMUNITY

DRAFT
EAC LEGAL FRAMEWORK FOR CYBERLAWS

November 2008

Table of Contents

Executive summary

The Framework for Cyberlaws ("Framework") was prepared by the East African Community EAC Task Force on Cyberlaws, comprising representatives from the Partner States and the EAC Secretariat, with the support of UNCTAD. The Framework contains a series of Recommendations made to the governments of the Partner States about reforming national laws to facilitate electronic commerce; to facilitate the use of data security mechanisms; to deter conduct designed to undermine the confidentiality, integrity and availability of information and communication technologies; to protect consumers in an online environment, and to protect individual privacy. The Recommendations are designed to harmonise the law reform process between the EAC Partner States, as well as reflecting international best practice.

1. Introduction

1.1 Background

The vision of regional integration in East Africa is to create wealth, raise the living standards of all people of East Africa and enhance international competitiveness of the region. The key to achieving this vision is increased production, trade and investments in the region with Information and Communication Technologies (ICT) playing a leading role. The information and knowledge-exchange driven third millennium requires reliable ICT services as a key national and regional resource. Furthermore, the EAC Treaty emphasises co-operation to achieve coordinated, harmonized, and complementary infrastructural development.

In this context, the EAC has recognized the need for implementing a Regional e-Government Programme considered as an important step towards deepening East African regional integration through the online provision of government information and services. The Programme aims to improve and enhance public services delivery through use of ICT in public administrations of the Partner States combined with organizational change and development of new skills. The improved public services delivery would in turn support regional integration for economic development of the region. Since 2004, three regional EAC workshops identified cyberlaws, e-justice and as well as information security as key cross cutting issues that need to be in place for a successful implementation of e-government applications and development of e-commerce in East Africa. [1] Further recommendations included that the EAC should ensure necessary coordination intended to harmonize regional and national legal frameworks. The Regional e-Government Framework adopted by the Council of Ministers in November 2006 identified the creation of an enabling legal and regulatory environment as a critical enabling factor for effective implementation of e-Government strategies at national and regional levels. It further emphasized that operational efficiency of any e-Government strategy need a strong back up support of necessary legislation on data security, network security, cyber crime, information systems and electronic transactions.

[1] Regional e-Government Framework Stakeholders Consultative meeting (28 - 29th June 2005); Workshop on Cyberlaws and e-Justice (on 25th –26th April 2006); Workshop on Information Security (27th –28th April 2006).

To support the implementation of the EAC Regional Government Programme, the EAC secretariat requested UNCTAD to build capacity for policy and legal experts from the Partner States and officers from the EAC. A first training workshop on "The Legal Aspects of e- Commerce" was jointly organized by the EAC and UNCTAD secretariats (Kenya**,** December 2006). The training workshop aimed at preparing lawmakers and government officials in all aspects to be considered for drafting cyberlaws and at promoting the development of a harmonized legal framework at the regional level. Following the defined roadmap toward a harmonised legal framework in the EAC prepared during this training workshop, the EAC Partner States appointed members to the Regional Task Force on Cyberlaws ("Task Force") formed in December 2007. The Task Force is drawn from Partner States Ministries and government departments; from regional associations of legal professionals (East African Law Society, East African Magistrates & Judges, East African Business Council); and from the EAC Secretariat (EAC Secretariat Legal Department, East African Court of Justice, East African Legislative Assembly).

UNCTAD facilitated the three meetings of the EAC Task Force held in 2008[2] which discussed possible options and challenges in the development of a harmonized regional legal framework. UNCTAD carried out a review of the existing draft laws and bills and assisted in the preparation of the following legal framework for harmonization of cyberlaws in the region.

1.2 Approach and Methodology

A participatory approach and consultative methodology was followed to gather from and share with information from the five Partner States namely Kenya, Uganda, Tanzania, Rwanda and Burundi which are at different stages of developing their domestic cyberlaws. As of September 2008, *Uganda* has prepared three bills that had been approved by the cabinet and were due to be presented to parliament for debate and enactment namely: Electronic Transactions Bill; Digital Signatures Bill; and Computer Misuse Bill. *Kenya* has a draft Electronic Transactions Bill covering aspects of legal recognition of e-documents and transactions. The Bill provides for among other things the institutional arrangements, offences, dispute resolution mechanism and safeguards for privacy and data protection. *Rwanda* has a draft bill providing for an omnibus law, covering electronic transactions and signatures, with similarities with the draft bills of Uganda and Kenya. *Tanzania* has no specific cyberlaw but there are various reform initiatives towards the enactment of the cyberlaws. In 2005, the Law Reform Commission of Tanzania submitted a report with recommendations on the Legal framework for e-commerce and cyber crimes. In 2007 Tanzania amended the Evidence Act to recognize electronic evidence. *Burundi* is yet to develop its cyberlaws.

Consultative meetings were held with regional Task Force members to collect information on current activities, requirements and identify challenges and opportunities in developing the Legal framework on Cyberlaws. A comparative analysis of the Commonwealth Model Law on Electronic Transactions (2002), the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures, and the

[2] First Meeting of the EAC Task Force on cyberlaws, January 2008, Arusha, Tanzania; Second Meeting of the EAC Task Force on cyberlaws, June 2008, Kampala, Uganda; Third Meeting of the EAC Task Force on cyberlaws, September 2008, Bujumbura, Burundi

SADC Model Cyberlaw has been carried out and found to be of relevance to EAC Partner States as a building block for harmonisation of cyberlaw initiatives.

In January 2008, the EAC held its first regional Task Force meeting on Cyberlaws in Arusha, Tanzania. At the meeting, attendees from four EAC member states, Burundi, Kenya, Uganda and Tanzania, discussed a range of issues relating to the need to reform national laws to address the increasing use of the Internet as a medium for electronic commerce and administration. The Task Force noted and commended that the process of law reform be co-ordinated at a regional level and harmonised and benchmarked against international best practice. The Task Force also recommended that a comparative review of the existing laws and bills of Partner States be undertaken and a regional legal framework be developed for harmonisation of cyberlaws.

In terms of developing a draft legal framework for EAC Partner States, the Task Force recommended that the process of reform be divided into two phases. In Phase I, cyberlaw reforms would focus on five key topics: Electronic transactions, electronic signature and authentication, data protection and privacy, consumer protection and computer crime. Phase II would address topics, such as intellectual property and taxation, which although impacting on cyberspace activities, were beyond the scope of the Task Force.

In May 2008, a draft legal framework was prepared for consideration and discussion at national consultative meetings. Feedback from these consultations was presented at the next meeting of the Task Force, held in Kampala, Uganda, in June 2008. The members of the Task Force then examined and debated the draft in detail and provided further input, as well identifying the key principles and issues in respect of each of the five subject areas.

In September 2008, the third meeting of the Task Force was held in Bujumbura, Burundi. The following text represents the outcome of these consultations and discussions. The document comprises a brief overview of the range of subject matter addressed within the proposed legal framework and a series of recommendations that the Task Force on Cyberlaws would like to make to the Partner States of the EAC, as well as to the EAC Secretariat, for consideration at both a national and regional level, as a means of promoting harmonised law reform to facilitate the use of electronic commerce and deter those that may wish to engage in unlawful conduct.

2. Legal Framework and Recommendations

The purpose of developing a Cyberlaw Framework for the EAC Partner States is to promote regional harmonisation in the legal response to the challenges raised by the increasing use and reliance on ICT for commercial and administrative activities, specifically in an Internet or cyberspace environment. Such a Framework details those agreed features that should be transposed into national laws and regulations in order to address the various issues identified in respect of the five topics discussed below. These features will include matters that are considered part of an essential response to a specific problem, as well as matters on which the Partner States may optionally choose to adopt measures.

The Framework also reflects international best practice and the existence of model laws and other instruments of public international law in each area of concern. However, the Framework is not itself a model law, thereby focusing the debate within the Task Force on the nature of the provisions being recommended to Partner States and avoiding the need for detailed scrutiny of specific draft provisions. This approach reflects not only the progress of the law reform process already underway within certain Partner States, but is also a pragmatic response to the work that has already been carried out in various forums and intergovernmental organisations.

The following discussed the areas in which it is recommended that legal provisions are adopted. Each topic is considered separately, although a Partner State may obviously, for reasons of legislative efficiency, decide to develop a draft bill addressing one or more topic. Where measures address more than one topic, however, it should be borne in mind that the nature of the political debate generated by each topic can differ considerably, such that controversy and resistance to the adoption of provisions on one topic may impact adversely on the adoption of the whole package of law reform proposals. For example, measures facilitating electronic transactions, could be less controversial than measures enhancing authority in the investigation of computer crime.

2.1 Electronic transactions

The overriding objective of a measure on electronic transactions is to facilitate the use of electronic means of communication to enter into and execute legal acts. The range of acts covered by the term ‘electronic transactions’ are not confined to commercial agreements for the purchase goods, products or services, but also encompasses interactions with government and administrative bodies, in either a commercial or non-commercial context.

2.1.1 General provisions

As with any legislative measure, there are certain matters that need to be addressed at the outset to aid interpretation and implementation of the measure. This section highlights four such issues: purpose and policy; sphere of application; variation and statutory definitions.

When adopting a measure on electronic transactions, governments have certain aims and objectives that the measure is intended to achieve. Such policy objectives can be expressly stated in the legislative instrument, e.g.:

> (a) To facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
>
> (b) To encourage the use of reliable forms of electronic commerce;
>
> (c) To facilitate electronic filing of documents with Government and to promote efficient delivery of Government services by means of reliable forms of electronic communications;

(d) To promote public confidence in the authenticity, integrity and reliability of data messages and electronic communications.

Such wording can serve to guide interpretation of a provision, particularly by a court or arbitrator, in the event of a dispute. Rather than leaving a provision to be interpreted literally, which may give rise to unintended consequence, reference to a purposive provision should guide interpretation in supportive manner. **The Task Force recommends the preparation and adoption of such purposive provisions (R. 1).**

The nature of the subject matter addressed in electronic commerce laws means that the impact may be horizontal across all sectors of business and the private sector, as well as public administrations. While such a broad scope may be welcomed, it may not always be appropriate in the circumstances. The legislation may, therefore, include a provision specifically detailing the areas in which the law is intended to apply. In general, for example, there will be a desire for it to be applicable in areas of civil and commercial law. Electronic transactions laws are not generally applicable to the field of criminal area, particularly criminal procedure, since this may have unintended consequences. It will be a matter of policy as to whether the law will extend to administrative acts carried out by public authorities. Even in those areas where the law does apply, explicit recognition may be given to the fact that there are exemptions, either on the face of the law or arising under general principles already present under national law. **The Task Force recommends that any electronic transaction law be generally applicable to all civil and administrative law matters (R.2).**

While governments may wish to extend the application of the law as widely as possible, subject to the express exemptions, such application may not always be appropriate or anticipated by the drafters. As such, it is recommended that the parties to an electronic transaction have the right to vary the provisions of the law through private agreement. While such agreements should not be capable of undermining the general thrust of the measure, or cause some other forms of harm, such as to consumers, the parties should be given the freedom to derogate by mutual agreement on certain matters. **The Task Force recommends that private entities be given the freedom to depart from the provisions of the electronic transactions law by agreement, in specified circumstances (R.3).**

As with most areas of law and regulation, a necessary first step is to define certain key terms used in the body of the instrument. Such definitions aid interpretation in the event of a dispute, especially when a term has multiple meanings that vary according to context. In a technology environment, there is also the need to provide some explanation to the potential audience, such as trading partners or the judiciary. A failure to supply satisfactory definitions may undermine one purpose of the measures, i.e. to reduce legal uncertainty and therefore facilitate the activity. The terms defined in electronic transaction laws tend to include the designation of certain *persons*, e.g. the ‘addressee’ and the ‘originator’ of an electronic communication, which has legal consequences; certain *technological concepts*, e.g. an ‘information system’, to distinguish it from other subject matter, such as computer data, and certain *activities*, e.g. the issuance of certificates in a digital signature environment. **The Task Force**

recommends that a comprehensive set of statutory definitions be incorporated in the electronic transactions legislation (R.4).

2.1.2 Issues of validity

The central issue addressed in an electronic transactions law concerns the validity of electronic communications as a means of executing a range of legal acts. Generally, such validity concerns arise in three distinct though related categories, each of which will generally be addressed in an electronic transaction law: Requirements of form, contract formation and record-keeping and evidential requirements.

- Requirements of form

Legal and regulatory systems abound with terms and phrases that, while not expressly excluding the use of electronic communications, were clearly used in reference to physical documents and processes, such that uncertainties exist whether electronic alternatives are acceptable. The three concepts most commonly seen as creating potential problems for electronic commerce are requirements for a legal act to be executed 'in writing'; that a document be 'signed', or that an 'original' be presented or retained. These requirements often also overlap, e.g. a writing must be signed.

In terms of responding to these requirements in an electronic commerce environment, it may be decided to take one of three possible courses of action. Firstly, *removal*, it may be decided that the requirement is no longer necessary, reflecting an environment or concern no longer present or relevant. In such circumstances, it would be preferable if the requirement was removed, although this may represent a substantial burden in terms of law reform, which could take a considerable period of time. Second, *preservation*, the need for the requirement may be viewed as continuing to be necessary and that the replacement with electronic alternatives should not be acceptable. As such, the electronic commerce law may expressly exclude its application in specified area, as discussed above. The third, and most common, approach is to *liberalise*, accepting that electronic communications should be capable of substituting for paper provided that the electronic replacement can exhibit the same or similar functionalities as those represented by the requirement in the first place, such as an evidential function.

Provisions should be drafted recognising the validity of electronic communications as meeting as requirement for a 'writing', 'signature' or 'original' and all areas where the law requires a person to file paper documents with public bodies including licensing, certification. Such validity may be subject to certain conditions being met and exemptions may be made for certain specified legal acts. The Task Force recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).[3] (R.5).

- Contract formation

[3] Article 9.

The use of data messages to form contracts may raise numerous questions that can be expressly addressed in an electronic transactions law. First, is such a contract valid? Some types of contracts are subject to specific requirements of form, designed to protect particular interests or persons, as discussed in the previous section. While national law may permit certain types of contract to be formed electronically, in the same way that oral contracts has been recognised as valid in many legal systems, for other it may be required that they continue to be executed in physical form, e.g. wills concerning succession.

Second, can a data message be viewed as the expression of a party's will (a requirement in many jurisdictions), especially where there has been no human review or intervention? eCommerce applications, such as the transactional webs sites, will often enable the information system to carry out all aspects of the contract formation process without any human intervention. As such, doubts may be raised as to whether such contracts exhibit an expression of the party's will. Express provision can recognise the validity of such completely automated processes, although it is only required where national contract law includes such a requirement.

Third, what terms are incorporated into the contract? Traditional contract law generally enables the incorporation of terms by reference, provided the party asserting such terms has given the other party an opportunity to refer to such terms prior to contract formation. In a web transaction environment, there may be uncertainty whether techniques such as hypertext links satisfy the requirements of law. Express reference in an electronic transactions law can therefore mitigate any such uncertainty.

Fourth, when and where can a contract be deemed to have been formed? While strictly an issue of contract formation, issues of when and where something occurs are generally addressed under separate provision in respect of the communication process.

The Task Force recommends that these issues of contract law be expressly addressed in the electronic transactions law and recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005)[4] (R.6).

- Record-keeping and evidential requirements

Many of the advantages of eCommerce techniques (including the ability to keep large amounts of information electronically for storage, searching and manipulation) are lost if a business is required to keep paper copies of every document or communication. Yet, legal systems often require businesses to retain certain records, and particularly written records, for accounting, revenue or audit purposes for a given period of time, often reflecting the needs of public administrations. In addition, organisations will retain records for evidential purposes, such as during the period in which a contractual or tortious action may be brought under national limitation statutes, or to evidence ownership of intellectual property rights. Many of these requirements are written in such a way that they appear to contemplate retention of a

[4] Articles 8, 11-13.

writing, or piece of paper. Consequently, the issue understandably arises as the ability to satisfy these record retention requirements in an electronic environment.

As with the requirements of form, a liberalising approach would be to accept electronic records provided they exhibit similar capabilities to those of traditional paper documents. So, for example, the message need not be retained unaltered as long as the information stored accurately reflects the information that was sent. Since electronic messages are often decoded, compressed or converted prior to storage, it would not be appropriate to require that information should be stored unaltered.

Closely related to national record-keeping requirements, an important issue in electronic commerce is whether, if a dispute were to arise, a court of law or tribunal in a jurisdiction would permit the proof of a fact through a data message? Under evidential rules in most jurisdictions, a distinction is made between:

- Whether the document can be submitted into court as evidence (the question of 'admissibility') and

- Whether the document will be considered good evidence of the facts it records (the question of evidential weight).

A number of jurisdictions have a highly formalised and strict system of evidentiary admissibility. Some require that evidence presented in a court of law must be in the form of a notarised document. Other countries impose a burden upon the party adducing the computer-derived evidence into court to show that the systems from which the evidence was derived were 'operating properly'; sometime a difficult threshold to meet, potentially requiring the use of numerous experts to explain to a court the technical aspects of each component of the system. To ensure that a party may be able to enforce its legal rights embodied in an electronic contract, such jurisdictions must provide for the admissibility of electronic evidence, such as electronic copies or printouts of electronic evidence, in its electronic transactions legislation.

One aspect of admissibility which arises in some common law legal systems is the concept of 'best evidence'. 'Best evidence' generally requires that a party adduce the best evidence available to it, i.e. an original should be submitted rather than a copy. This historic rule has generated some legal uncertainty in respect of data messages, since the concept of an 'original' has little meaning in an electronic commerce environment. Express provision may therefore state that electronic evidence such not be inadmissible if it is the best evidence that the party adducing it could be reasonably be expected to produce.

Having established the admissibility of electronic evidence, the second question is the weight to be given to the evidence. Legislative provision may list factors that a court should use in assessing the evidential weight, such as the reliability of the manner in which the data message was generated, stored or communicated, the integrity of the information contained in the data message was maintained, and the manner in which the originator of the data message is identified. In some jurisdictions, standards have been developed for the secure operation of electronic systems, designed to facilitate their use as evidence in the event of a dispute.

The Task Force recommends that the electronic transaction law facilitates electronic record-keeping and permits the admission of electronic records as evidence before a judicial, administrative or dispute resolution body, subject to certain conditions (R.7).

The Task Force recommends that regional standards be developed, reflecting international standards, to assist judicial, administrative or dispute resolution bodies to evaluate the evidential value of electronic records (R.8).

2.1.3 Communications Process

One of the most significant characteristics of eCommerce is that geographic boundaries become irrelevant: people throughout the world can communicate quickly and easily, and many times may do so without knowledge of the location of the other party. While geography may be irrelevant for eCommerce, however, geography – and particularly the *place* where certain acts such as the dispatch or receipt of a communication occur – is still relevant to several legal issues in such areas as private international law (i.e. choice of law and forum) or contract creation. Moreover, determining the place of dispatch or receipt raises a variety of questions: is the message sent when the "send" button is pushed, or is something else needed? Is a message received when my server receives it, it is put in my mailbox, I download it, or I read it? These and similar questions require a clear, and consistent, answer. Therefore, many electronic transaction laws contain provisions defining *when* and *where* dispatch and receipt occur.

The question of "when" something is sent or received is generally determined by reference to whether the message is within the sphere controlled by the sender or the recipient. Thus, dispatch occurs when the message "enters an information system outside the control" of the sender. Similarly, where the recipient has designated a certain information system for receipt of messages, receipt occurs when the message enters that information system. However, if the recipient has not designated any such information system, no receipt occurs until the recipient actually receives it.

Addressing the "where" issue is more complicated. The difficulty with "where" something occurs is that the physical location of the parties at any relevant time (particularly with laptop usage combined with cellular or wireless technology) may not only constantly be changing, but may be unknown. Thus, any relationship between a person's location and the underlying transaction may be entirely fortuitous. Moreover, the location of the computers or systems processing the information, e.g. a web server, may be equally irrelevant to the transaction. As a result, a data message is deemed dispatched at the place where the sender has its place of business, and is deemed received at the place where the recipient has its place of business. Both these locations are comparatively easy to lay down in law.

The Task Force recommends that the electronic transactions law addresses the issue of when and where an electronic communication is sent and received, and

recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005)[5] (R.9).

2.1.4 Government acts and transactions

Many of the requirements that things be done using pieces of paper are found not in statute but in administrative rules and regulations, i.e. existing custom and practice. The acceptance of electronic alternatives requires as much a cultural shift within the practices of public authorities, as it does require amendments in the law. However, explicit recognition of the role of government and public administrations in the validity of electronic transactions in law can serve to facilitate such a cultural shift. The objective of facilitating eGovernment could be a stated objective at the commencement of the law.

It must also be recognised that a simple liberalisation scheme may not be appropriate across the range of administrative functions being carried out and therefore an authority should have reserve powers to specify certain requirements in respect of electronic communications. While it seems appropriate to encourage governments and administrations to accept electronic communications, requiring that private entities and individuals accept electronic communications from governments or public authorities would seem an inappropriate imposition.

The Task Force recommends that specific provision be made in any electronic transaction law stating that public authorities should accept electronic modes of communication (R.10).

2.1.5 Liability issues

Where illegal content is made accessible over the Internet in contravention of applicable national rules, states will often require a Internet service provider (ISP) to hand over any details which may establish the real-world identity of the content provider. The ISP is also often required to remove the illegal content and any links to it that have been found to exist on its servers. As one of the key purposes of content regulation is to ensure that certain kinds of information are not available to the general public, such requirements can be used in an effort to make sure that content regulation is enforced even if the provider of the illegal content cannot be identified and prosecuted.

However, a key question that arises in relation to the role of ISPs is whether they may be held liable in respect of the third-party content that they may provide access to, cache, or host, without knowledge? If ISPs were to be held liable for all content to which they provide access, then they are less likely to offer such services, which would be to the detriment of the development of eCommerce.

As a consequence, many states provide ISPs with certain immunity from civil and criminal liability for third-party content, to the extent that they are simply providing a communication or storage service and are not responsible for, or are not aware, of the illegal nature of such content. Once an ISP becomes aware or has knowledge of the

[5] Article 10.

illegal nature of the content, when notified by a user or a relevant authority, then the ISP would be expected to remove or disable access to such content promptly in order to preserve their immunity, until such time as a determination is made as to the legality of the content.

The Task Force recommends that Partner States give consideration to the adoption of rules to protect communication intermediaries from liability for third-party content, subject to certain conditions (R.11).

2.1.6 Institutional implications

The Task Force recognises that as a facilitating measure, the electronic transactions law is likely to have a more significant impact and be adopted more rapidly and widely by business, consumers and administrative bodies if responsibility for implementation of the law was given to a relevant national agency, which could champion use of the law.

In order for the EAC to keep abreast and take advantage of emerging opportunities in cyberspace, the Task Force recommends that

- **Partner States should endeavour to research and implement institutional reforms to provide for policy formulation, implementation, regulations and private sector participation;**
- **Consideration is given to institutional reforms at the EAC Secretarial level to carry forward emerging challenges in legal framework with respect to cyberlaw issues (R.12).**

2.2 Electronic Signatures and Authentication

As noted above, electronic signatures raise two distinct issues; whether they are valid in terms of meeting requirements for the use of a 'signature', and whether they can appropriately authenticate the party executing the signature and ensure the integrity of the contents of the document to which the signature relates. The former issue of validity has been addressed in section 4.1 above. The latter concerns the security functionality of the signature process. There are inevitably concerns that electronic communications may not be sufficiently secure, such that someone may pretend to be someone they are not or amend the content of a document in a manner that is difficult if not impossible to discern. To what extent is it therefore appropriate to specifically address the security of electronic signatures in an electronic transaction law?

Over recent years, considerable attention has been given to the possible use of digital signatures, using public-key cryptography, often supported through the use of third party certificates that verify that the sender is the legitimate holder of the relevant key. In some jurisdictions, this technology and methodology has been given express recognition in primary legislation, such as electronic transactions legislation. Such legislation details the criteria that the electronic signature should meet if it is to be given legal recognition and conferred with beneficial legal presumptions.

The criteria that an electronic signature is expected to meet in order to be accepted in law as functionally equivalent to a traditional handwritten signature will sometimes

include the use of a certificate issued by a third party certification authority or service provider, similar in nature to the services provided by notary publics in EAC member states. Due to the critical role of such entities in the security of the process, the legislation will often establish a regulatory framework governing the provision of such services. This framework may include a licensing or accreditation scheme designed to control market entry. In addition, a raft of criteria will be laid down concerning the manner in which the service provider operates, including the attribution of liability in the event of a failure to meet the criteria.

Experience of such regimes to date, however, suggests that they are very complex and difficult to implement and operate. As such, they have often proven unable to facilitate secure electronic transactions.

The Task Force recommends that Partner States give consideration to granting delegated authority to a specified government ministry or department to adopt relevant secondary regulations concerning digital signatures and the provision of certification services (R.13).

The Task Force makes the following additional recommendations in respect of electronic signatures:

- **That Partner States provide for a statutory definition for 'signatures' and 'electronic signatures'**

- **That Partner States should support the principle of technology neutrality and promote interoperability in respect of 'electronic signatures' technologies**

- **That Partner States should identify and recognise internationally standards in relation to the use and operation of electronic signatures**

- **That Partner States should consider the need for an institutional framework to support the provision of certification and related services at both a national and regional level (R.14).**

2.3 Cybercrime

Generally legislative initiatives in the area of computer or cybercrime have two distinct objectives. First, there is a need to amend or supplement existing criminal law to reflect the use of ICTs to commit a range of traditional offences or to engage in undesirable acts against ICTs and the data they process. Second, there is a need to reform criminal procedure rules to facilitate the investigation and prosecution of those that engage in criminal acts using or against ICTs by law enforcement agencies.

The Task Force recommends that Partner States should undertake reform of their criminal laws to specifically provide for cybercrimes (R. 15).

2.3.1 Substantive offences

Where ICTs are used as a tool to commit a traditional offence, there may be a need to amend existing criminal provisions to reflect the use of such technologies. Under the Council of Europe Cybercrime Convention (2001), offences in relation to fraud forgery, infringements of intellectual property rights and child pornography are all recast to take into account the use of ICTs in their commission.

The Task Force recommends that the impact of ICTs on criminal conduct be given due consideration whenever a Partner State engages in a review or examination of its criminal code in the course of a reform initiative (R.16).

In terms of offences targeting the confidentiality, integrity and availability of computer or information systems and the data they process, there is broad consensus around the types of conduct that should be criminalised:

- Unauthorised access to the system
- Unauthorised interference or modification of the system or the data processed on the system
- Unauthorised interception of communications between or within systems;
- Misuse of devices, including the supply or possession of tools such as password cracking or virus writing software.

Measures designed to tackle cyber-terrorist or cyber-warfare conduct are based around the motivation of the offender rather than his conduct, which will generally fall within one of the four categories above. Similarly, spamming, the mass sending of unsolicited emails, is not itself an offence in most jurisdictions, although it will often involve the commission of computer integrity offences in the course of its commission, such as creating a 'zombie' computer from which to send the messages.

The jurisdictional scope of these offences will generally be extended to capture both conduct carried out in the territory, where the harm or victim resides in another jurisdiction; as well as when the victim or harm occurs within the territory. Consideration may also be given to whether extra-territorial jurisdiction should be provided for, where the conduct, victim and harm occur outside of the territory, but the perpetrator is a national of the jurisdiction.

2.3.2 Criminal procedure

While the impetus for reform of criminal procedure and the powers of law enforcement agencies may be driven by concerns about cybercrime, it must be borne in mind that the reformed regime will generally be applicable across all forms of criminality. As such, new powers that may be seen as desirable to tackle a particular instance of cyber-criminality may appear excessive in a broader context of criminal investigation.

It is often necessary that measures be taken to address the abilities and capabilities of law enforcement agencies to obtain and access forensic data when being stored on a system or device and when being transmitted between devices. In the former situation, this will include amending the concept of search and seizure, particularly where the evidence is held remotely but within the same jurisdiction. Obtaining access to data protected through encryption or other techniques may also require specific legislative

provision, placing an obligation upon the perpetrator to disclose information necessary to render the evidence intelligible.

Laws permitting law enforcement interception of communications in the course of a criminal investigation are generally already present in most jurisdictions; however, such laws may require review and amendment to reflect modern communication techniques. In particular, obligations may need to be placed upon telecommunication providers to assist law enforcement agencies in obtaining access to both stored data and data in the course of transmission.

The Task Force recommends the following:

- **That Partner States undertake reform of substantive and procedural criminal laws to address the phenomenon of computer crime.**

- **That the EAC Secretariat considers the possible role of the Court of Justice in addressing the multi-jurisdictional nature of computer crime and the adoption of common criminal procedures within the EAC.**

- **That Partner States give due consideration to the wording and provisions of the Council of Europe Convention on Cybercrime (2001)[6].**

- **That the EAC Secretariat and the Partner States examine the possibility of acceding to the Council of Europe Convention on Cybercrime (2001)[7] (R.17).**

2.4 Consumer Protection

Existing consumer protection laws will often encompass Internet-based transactions without the need for amendment; while consumer protection measures addressing such transactions only make sense within a broader consumer protection framework. The objective of consumer protection rules in a cyberspace environment should be to facilitate eCommerce, from a demand-side, by engendering trust among consumers and thereby encouraging them to enter into online transactions. However, the imposition of substantial additional obligations upon online vendors should avoid becoming a legal obstacle to the provision of transactional activities.

The following measures have been widely adopted internationally to provide a clear level of protection for consumers in a cyberspace environment:

- Information requirements – Vendors should be obliged to make readily available to consumers a range of information concerning the identity of the vendor, the nature of the transactions, the process by which the transaction is entered into and all the associated costs to be paid by the consumers, including applicable taxes and delivery costs.

[6] See Annex II.
[7] See Article 37, 'Accession to the Convention'.

- Cancellation right – A consumer should be granted the right to cancel a contract for certain types of goods and services, without reason and within a specified time period.

- Payment fraud – A consumer should be granted certain protections from liability for fraudulent payments made in the consumer's name, unless the vendor or payment service provider can prove that the consumer has been grossly negligent in the operation of the payment mechanism.

- Performance obligations – The vendor should be obliged to perform the contract within a minimum specified period of time or be liable to fully refund the consumer.

In addition, existing rules governing the content and techniques used to advertise and market goods and services should be reviewed and amended to take into account innovative online mechanisms, such as 'pop-ups', that may fall outside the current regime.

The Task Force recommends the following:

- **That the EAC Secretariat and Partner States give due consideration to consumer protection issues in cyberspace within a broader consumer protection framework, at both a national and regional level.**

- **That reforms should encompass information requirements, cancellation rights, payment fraud and performance obligations.**

- **That the EAC Secretariat and Partner States initiate programmes to raise consumer awareness about the benefits and risks of transacting in cyberspace, including such things as labelling schemes.**

- **That the EAC Secretariat and Partner States give further consideration to the regional and national implications of electronic money or digital cash and the need to develop an appropriate regulatory framework (R.18).**

2.5 Data Protection and Privacy

For the purposes of the Framework, 'data protection' is used here to describe those obligations placed upon those entities that process information about living individuals, generally referred to as 'personal data'. A data protection regime will also grant certain rights upon individual data subjects.

The application of data protection rules may be limited only to private sector entities or public bodies. A sectoral regulatory response may be appropriate to address specific uses and abuses of personal data, whether driven by domestic or foreign concerns, such as the financial services sector.

In terms of the entity responsible for the processing, the following minimum obligations represent international best practice in the area:

- To comply with certain 'principles of good practice' in respect of their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security.

- To supply the individual with a copy of any personal data being held and processed and provide an opportunity for incorrect data to be amended.

The cost of regulation will be a critical factor in data protection. The cost associated with a comprehensive or omnibus approach, specifically the establishment of a dedicated regulatory authority, will generally be excessive for most developing countries, especially if borne by the private sector through licensing or notification fees. However, in terms of addressing privacy concerns vis-à-vis public sector infringements, an authority independent from government will generally be necessary in order to provide the necessary trust and assurance in its activities. The regulatory authority may not have an exclusively data protection remit, which mitigates the costs involved.

Whilst a self-regulatory or co-regulatory approach may be appealing in terms of minimising the public costs of regulation, its success depends on a sufficiently strong and active private sector, willing and able to fund the regulatory activity. It is also unlikely to be appropriate in terms of the public sector use of personal data.

The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area (R.19).

3. Conclusions and way forward

All the EAC Partner States have expressly recognised the need to address the legal and regulatory framework as one element of a national response to the promotion of ICTs and electronic commerce. In addition, there are numerous international and regional model instruments available to Partner States to guide them when drafting national legal measures that reflect best practice in the field, specifically those provided in the Annexes. However, the Task Force recognises the challenges faced by Partner States in order to successfully take the process of law reform from initial recognition of the issue and the preparation of draft measures to their formal adoption by the national political institutions and implementation in a manner that has a real impact on business and administrative attitudes and practices.

From experience in other jurisdictions, addressing the process of effective law reform will often involve a number of elements and steps. First, there is the need for express political commitment to the law reform process at the highest level of governments. Second, a relevant government ministry must claim ownership over the matter and be prepared to devote sufficient internal resources, both to carry out the necessary work internally as well as liaise and co-ordinate actively with other relevant stakeholders in the process, particularly other ministerial departments. A third element is the need to

identify and appoint relevant technical and legal expertise to support the lead ministry, internal to the authority and, or, external, whether located nationally or internationally. The work of the expert(s) must then be supported through the establishment of a stakeholder review group, chaired by the lead ministry, including representation from the public and private sectors. Obvious potential candidates include people from the ministry of justice, the national law reform commission and local commercial and legal practitioners. Any draft measures prepared by the experts would then be subjected to a process of scrutiny by the stakeholder review group, which should both substantially improve the quality of the final draft and facilitate awareness and build support for the proposal among the wider community. Finally, the draft measure should be steered through the parliamentary process by the lead ministry, ensuring that steps are taken to fully explain the purpose, nature and consequences of the measure to the political representatives.

In terms of the institutional implications of the Recommendations, the Task Force notes that preference should be given to identifying existing institutions to take on some of the proposed tasks, rather than establishing new entities with associated costs and time involved.

Envisaging law reform has always been substantially easier than achieving law reform. To successfully address the legal aspects of ICT development requires that EAC Partner States devote as much time and resources to the process of law reform as to the various subject matters identified in the Legal Framework.

Annex I: List of Recommendations

R.1 The Task Force recommends the preparation and adoption of such purposive provisions

R.2 The Task Force recommends that any electronic transaction law be generally applicable to all civil and administrative law matters.

R.3 The Task Force recommends that private entities be given the freedom to depart from the provisions of the electronic transactions law by agreement, in specified circumstances.

R.4 The Task Force recommends that a comprehensive set of statutory definitions be incorporated in the electronic transactions legislation.

R.5 Provisions should be drafted recognising the validity of electronic communications as meeting as requirement for a 'writing', 'signature' or 'original' and all areas where the law requires a person to file paper documents with public bodies including licensing, certification. Such validity may be subject to certain conditions being met and exemptions may be made for certain specified legal acts. The Task Force recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

R.6 The Task Force recommends that these issues of contract law be expressly addressed in the electronic transactions law and recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

R.7 The Task Force recommends that the electronic transaction law facilitates electronic record-keeping and permits the admission of electronic records as evidence before a judicial, administrative or dispute resolution body, subject to certain conditions.

R.8 The Task Force recommends that regional standards be developed, reflecting international standards, to assist judicial, administrative or dispute resolution bodies to evaluate the evidential value of electronic records.

R.9 The Task Force recommends that the electronic transactions law addresses the issue of when and where an electronic communication is sent and received, and recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

R.10 The Task Force recommends that specific provision be made in any electronic transaction law stating that public authorities should accept electronic modes of communication.

R.11 The Task Force recommends that Partner States give consideration to the adoption of rules to protect communication intermediaries from liability for third-party content, subject to certain conditions.

R.12 In order for the EAC to keep abreast and take advantage of emerging opportunities in cyberspace, the Task Force recommends that

- Partner States should endeavour to research and implement institutional reforms to provide for policy formulation, implementation, regulations and private sector participation.

- Consideration is given to institutional reforms at the EAC Secretarial level to carry forward emerging challenges in legal framework with respect to cyberlaw issues.

R.13 The Task Force recommends that Partner States give consideration to granting delegated authority to a specified government ministry or department to adopt relevant secondary regulations concerning digital signatures and the provision of certification services.

R.14 The Task Force makes the following additional recommendations in respect of electronic signatures:

- That Partner States provide for a statutory definition for ‘signatures’ and ‘electronic signatures’

- That Partner States should support the principle of technology neutrality and promote interoperability in respect of ‘electronic signatures’ technologies

- That Partner States should identify and recognise internationally standards in relation to the use and operation of electronic signatures

- That Partner States should consider the need for an institutional framework to support the provision of certification and related services at both a national and regional level.

R.15 The Task Force recommends that Partner States should undertake reform of their criminal laws to specifically provide for cybercrimes.

R.16 The Task Force recommends that the impact of ICTs on criminal conduct be given due consideration whenever a Partner State engages in a review or examination of its criminal code in the course of a reform initiative.

R.17 The Task Force recommends the following:

- That Partner States undertake reform of substantive and procedural criminal laws to address the phenomenon of computer crime.

- That the EAC Secretariat considers the possible role of the Court of Justice in addressing the multi-jurisdictional nature of computer crime and the adoption of common criminal procedures within the EAC.

- That Partner States give due consideration to the wording and provisions of the Council of Europe Convention on Cybercrime (2001).

- That the EAC Secretariat and the Partner States examine the possibility of acceding to the Council of Europe Convention on Cybercrime (2001).

R.18 The Task Force recommends the following:

- That the EAC Secretariat and Partner States give due consideration to consumer protection issues in cyberspace within a broader consumer protection framework, at both a national and regional level.

- That reforms should encompass information requirements, cancellation rights, payment fraud and performance obligations.

- That the EAC Secretariat and Partner States initiate programmes to raise consumer awareness about the benefits and risks of transacting in cyberspace, including such things as labelling schemes.

- That the EAC Secretariat and Partner States give further consideration to the regional and national implications of electronic money or digital cash and the need to develop an appropriate regulatory framework.

R. 19 The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area.

Annex II: United Nations Convention on the Use of Electronic Communications in International Contracts (2005)

The States Parties to this Convention,

Reaffirming their belief that international trade on the basis of equality and mutual benefit is an important element in promoting friendly relations among States,

Noting that the increased use of electronic communications improves the efficiency of commercial activities, enhances trade connections and allows new access opportunities for previously remote parties and markets, thus playing a fundamental role in promoting trade and economic development, both domestically and internationally,

Considering that problems created by uncertainty as to the legal value of the use of electronic communications in international contracts constitute an obstacle to international trade,

Convinced that the adoption of uniform rules to remove obstacles to the use of electronic communications in international contracts, including obstacles that might result from the operation of existing international trade law instruments, would enhance legal certainty and commercial predictability for international contracts and help States gain access to modern trade routes,

Being of the opinion that uniform rules should respect the freedom of parties to choose appropriate media and technologies, taking account of the principles of technological neutrality and functional equivalence, to the extent that the means chosen by the parties comply with the purpose of the relevant rules of law,

Desiring to provide a common solution to remove legal obstacles to the use of electronic communications in a manner acceptable to States with different legal, social and economic systems,

Have agreed as follows:

Chapter I

Sphere of application

Article 1

Scope of application

1. This Convention applies to the use of electronic communications in connection with the formation or performance of a contract between parties whose places of business are in different States.

2. The fact that the parties have their places of business in different States is to be disregarded whenever this fact does not appear either from the contract or from any

dealings between the parties or from information disclosed by the parties at any time before or at the conclusion of the contract.

3. Neither the nationality of the parties nor the civil or commercial character of the parties or of the contract is to be taken into consideration in determining the application of this Convention.

Article 2

Exclusions

1. This Convention does not apply to electronic communications relating to any of the following:

    (a) Contracts concluded for personal, family or household purposes;
    (b) (i) Transactions on a regulated exchange; (ii) foreign exchange transactions; (iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; (iv) the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary.

1. This Convention does not apply to bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money.

Article 3

Party autonomy

The parties may exclude the application of this Convention or derogate from or vary the effect of any of its provisions.

Chapter II

General provisions

Article 4

Definitions

For the purposes of this Convention:

(a) “Communication” means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract;

(b) “Electronic communication” means any communication that the parties make by means of data messages;

(c) “Data message” means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy;

(d) “Originator” of an electronic communication means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but it does not include a party acting as an intermediary with respect to that electronic communication;

(e) “Addressee” of an electronic communication means a party who is intended by the originator to receive the electronic communication, but does not include a party acting as an intermediary with respect to that electronic communication;

(f) “Information system” means a system for generating, sending, receiving, storing or otherwise processing data messages;

(g) “Automated message system” means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the system;

(h) “Place of business” means any place where a party maintains a nontransitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location.

Article 5

Interpretation

1. In the interpretation of this Convention, regard is to be had to its international character and to the need to promote uniformity in its application and the observance of good faith in international trade.

2. Questions concerning matters governed by this Convention which are not expressly settled in it are to be settled in conformity with the general principles on which it is based or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law.

Article 6

Location of the parties

1. For the purposes of this Convention, a party’s place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.

2. If a party has not indicated a place of business and has more than one place of business, then the place of business for the purposes of this Convention is that which has the closest relationship to the relevant contract, having regard to the

circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract.

3. If a natural person does not have a place of business, reference is to be made to the person's habitual residence.

4. A location is not a place of business merely because that is: (a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (b) where the information system may be accessed by other parties.

5. The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

Article 7

Information requirements

Nothing in this Convention affects the application of any rule of law that may require the parties to disclose their identities, places of business or other information, or relieves a party from the legal consequences of making inaccurate, incomplete or false statements in that regard.

Chapter III

Use of electronic communications in international contracts

Article 8

Legal recognition of electronic communications

1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.

2. Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct.

Article 9

Form requirements

1. Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.

2. Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.

3. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication;
and
(b) The method used is either:
(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

4. Where the law requires that a communication or a contract should be made available or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:

(a) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and
(b) Where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.

5. For the purposes of paragraph 4 (a):

(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and
(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

Article 10

Time and place of dispatch and receipt of electronic communications

1. The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the

addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with article 6.

4. Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.

Article 11

Invitations to make offers

A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

Article 12

Use of automated message systems for contract formation

A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

Article 13

Availability of contract terms

Nothing in this Convention affects the application of any rule of law that may require a party that negotiates some or all of the terms of a contract through the exchange of electronic communications to make available to the other party those electronic communications which contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.

Article 14

Error in electronic communications

1. Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made if:

(a) The person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and

(b) The person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.

2. Nothing in this article affects the application of any rule of law that may govern the consequences of any error other than as provided for in paragraph 1.

Chapter IV

Final provisions

Article 15

Depositary

The Secretary-General of the United Nations is hereby designated as the depositary for this Convention.

Article 16

Signature, ratification, acceptance or approval

1. This Convention is open for signature by all States at United Nations Headquarters in New York from 16 January 2006 to 16 January 2008.

2. This Convention is subject to ratification, acceptance or approval by the signatory States.

3. This Convention is open for accession by all States that are not signatory States as from the date it is open for signature.

4. Instruments of ratification, acceptance, approval and accession are to be deposited with the Secretary-General of the United Nations.

Article 17

Participation by regional economic integration organizations

1. A regional economic integration organization that is constituted by sovereign States and has competence over certain matters governed by this Convention may similarly sign, ratify, accept, approve or accede to this Convention. The regional economic integration organization shall in that case have the rights and obligations of a Contracting State, to the extent that that organization has competence over matters governed by this Convention. Where the number of Contracting States is relevant in this Convention, the regional economic integration organization shall not count as a Contracting State in addition to its member States that are Contracting States.

2. The regional economic integration organization shall, at the time of signature, ratification, acceptance, approval or accession, make a declaration to the depositary specifying the matters governed by this Convention in respect of which competence has been transferred to that organization by its member States. The regional economic integration organization shall promptly notify the depositary of any changes to the distribution of competence, including new transfers of competence, specified in the declaration under this paragraph.

3. Any reference to a "Contracting State" or "Contracting States" in this Convention applies equally to a regional economic integration organization where the context so requires.

4. This Convention shall not prevail over any conflicting rules of any regional economic integration organization as applicable to parties whose respective places of business are located in States members of any such organization, as set out by declaration made in accordance with article 21.

Article 18

Effect in domestic territorial units

1. If a Contracting State has two or more territorial units in which different systems of law are applicable in relation to the matters dealt with in this Convention, it may, at the time of signature, ratification, acceptance, approval or accession, declare that this Convention is to extend to all its territorial units or only to one or more of them, and may amend its declaration by submitting another declaration at any time.

2. These declarations are to be notified to the depositary and are to state expressly the territorial units to which the Convention extends.

3. If, by virtue of a declaration under this article, this Convention extends to one or more but not all of the territorial units of a Contracting State, and if the place of business of a party is located in that State, this place of business, for the purposes of this Convention, is considered not to be in a Contracting State, unless it is in a territorial unit to which the Convention extends.

4. If a Contracting State makes no declaration under paragraph 1 of this article, the Convention is to extend to all territorial units of that State.

Article 19

Declarations on the scope of application

1. Any Contracting State may declare, in accordance with article 21, that it will apply this Convention only:

(a) When the States referred to in article 1, paragraph 1, are Contracting States to this Convention; or
(b) When the parties have agreed that it applies.

2. Any Contracting State may exclude from the scope of application of this Convention the matters it specifies in a declaration made in accordance with article 21.

Article 20

Communications exchanged under other international conventions

1. The provisions of this Convention apply to the use of electronic communications in connection with the formation or performance of a contract to which any of the following international conventions, to which a Contracting State to this Convention is or may become a Contracting State, apply:

Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 10 June 1958);
Convention on the Limitation Period in the International Sale of Goods (New York, 14 June 1974) and Protocol thereto (Vienna, 11 April 1980);
United Nations Convention on Contracts for the International Sale of Goods (Vienna, 11 April 1980);
United Nations Convention on the Liability of Operators of Transport Terminals in International Trade (Vienna, 19 April 1991);
United Nations Convention on Independent Guarantees and Stand-by Letters of Credit (New York, 11 December 1995);
United Nations Convention on the Assignment of Receivables in International Trade (New York, 12 December 2001).

2. The provisions of this Convention apply further to electronic communications in connection with the formation or performance of a contract to which another international convention, treaty or agreement not specifically referred to in paragraph 1 of this article, and to which a Contracting State to this Convention is or may become a Contracting State, applies, unless the State has declared, in accordance with article 21, that it will not be bound by this paragraph.

3. A State that makes a declaration pursuant to paragraph 2 of this article may also declare that it will nevertheless apply the provisions of this Convention to the use of electronic communications in connection with the formation or performance of any contract to which a specified international convention, treaty or agreement applies to which the State is or may become a Contracting State.

4. Any State may declare that it will not apply the provisions of this Convention to the use of electronic communications in connection with the formation or performance of

a contract to which any international convention, treaty or agreement specified in that State's declaration, to which the State is or may become a Contracting State, applies, including any of the conventions referred to in paragraph 1 of this article, even if such State has not excluded the application of paragraph 2 of this article by a declaration made in accordance with article 21.

Article 21

Procedure and effects of declarations

1. Declarations under article 17, paragraph 4, article 19, paragraphs 1 and 2, and article 20, paragraphs 2, 3 and 4, may be made at any time. Declarations made at the time of signature are subject to confirmation upon ratification, acceptance or approval.

2. Declarations and their confirmations are to be in writing and to be formally notified to the depositary.

3. A declaration takes effect simultaneously with the entry into force of this Convention in respect of the State concerned. However, a declaration of which the depositary receives formal notification after such entry into force takes effect on the first day of the month following the expiration of six months after the date of its receipt by the depositary.

4. Any State that makes a declaration under this Convention may modify or withdraw it at any time by a formal notification in writing addressed to the depositary. The modification or withdrawal is to take effect on the first day of the notification by the depositary.

Article 22

Reservations

No reservations may be made under this Convention.

Article 23

Entry into force

1. This Convention enters into force on the first day of the month following the expiration of six months after the date of deposit of the third instrument of ratification, acceptance, approval or accession.

2. When a State ratifies, accepts, approves or accedes to this Convention after the deposit of the third instrument of ratification, acceptance, approval or accession, this Convention enters into force in respect of that State on the first day of the month following the expiration of six months after the date of the deposit of its instrument of ratification, acceptance, approval or accession.

Article 24

Time of application

This Convention and any declaration apply only to electronic communications that are made after the date when the Convention or the declaration enters into force or takes effect in respect of each Contracting State.

Article 25

Denunciations

1. A Contracting State may denounce this Convention by a formal notification in writing addressed to the depositary.

2. The denunciation takes effect on the first day of the month following the expiration of twelve months after the notification is received by the depositary. Where a longer period for the denunciation to take effect is specified in the notification, the denunciation takes effect upon the expiration of such longer period after the notification is received by the depositary.

DONE at New York, this […] day of […], 2005, in a single original, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic.
IN WITNESS WHEREOF the undersigned plenipotentiaries, being duly authorized by their respective Governments, have signed this Convention.

Annex III: Council of Europe Convention on Cybercrime (2001)

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.