Chapter I
General provisions

Article 1
Aims

The aims of this Convention are:

To promote the adoption and strengthening of measures to effectively prevent and combat ICT-related crimes and other illegal acts;

To prevent actions targeting the confidentiality, integrity and availability of ICT, and to prevent the misuse of ICT, by making punishable the acts covered by this Convention, and by providing powers sufficient to effectively combat such crimes and other illegal acts, by facilitating their detection, investigation and prosecution at both the domestic and international level and by developing arrangements for international cooperation;

To improve the efficiency of international cooperation, and to develop such cooperation, including in the area of training and the provision of technical assistance for preventing and combating ICT-related crimes.

Article 2
Scope of application

This Convention shall apply, in accordance with its provisions, to the prevention, detection, suppression, investigation and prosecution of the offences and other illegal acts recognized as such under articles 6–29 of this Convention and to the implementation of measures to eliminate the consequences of such acts, including the suspension of transactions relating to assets obtained as a result of the commission of any crime or other illegal act established as such under this Convention, and the seizure, confiscation and return of the proceeds of such crimes.

For the purposes of implementing this Convention, it shall not be necessary for the crimes and other illegal acts referred to in it to result in material damage, except as otherwise provided herein.

Article 3
Protection of sovereignty

1. The States parties shall carry out their obligations under this Convention in accordance with the principles of State sovereignty, the sovereign equality of States and non-interference in the internal affairs of other States.

2. This Convention shall not authorize the competent authorities of a State party to exercise in the territory of another State party the jurisdiction and functions that are reserved exclusively for the authorities of that other State under its domestic law, except as otherwise provided for in this Convention.

Article 4

Terms and definitions

For the purposes of this Convention:

(a) "Seizure of property" shall mean the temporary prohibition of the transfer, conversion, disposition or movement of property, or the temporary assumption of custody or control of property pursuant to an order of a court or other competent authority;

(b) "Botnet" shall mean two or more ICT devices on which malicious software has been installed and which are controlled centrally without the knowledge of users;

(c) "Malicious software" shall mean software the purpose of which is the unauthorized modification, destruction, copying, and blocking of information, or neutralization of software used to secure digital information;

(d) "Child pornography" shall have the meaning given to that term under article 2 (c) of the Optional Protocol of 25 May 2000 to the Convention on the Rights of the Child, on the sale of children, child prostitution and child pornography;

(e) "Proceeds" shall mean any property derived from or obtained, directly or indirectly, through the commission of any crime or other illegal act covered by this Convention, as well as income or other benefit derived from such proceeds, from property into which such proceeds have been transformed or converted or from property with which such proceeds have been intermingled;

(f) "Information and communications technologies" (ICT) shall mean processes and methods of generating, processing and distributing information, as well as ways and means of their implementation;

(g) "Information and telecommunications networks" shall mean a set of engineering equipment designed to control technological processes by means of computer technology and telecommunications;

(h) "Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including money in bank accounts, digital financial assets, digital currency, including cryptocurrency, and legal documents or instruments evidencing title to such assets or any part thereof;

(i) "Information" shall mean any data (messages, records), irrespective of the form in which it is presented;

(j) "Confiscation" shall mean the forcible deprivation of property without compensation pursuant to an order of a court or other competent authority;

(k) "Computer attack" shall mean the targeted interference of software and/or hardware and software with information systems or information and telecommunications networks to disrupt and/or terminate their functioning and/or threaten the security of information processed by such facilities;

(l) "Digital information" shall mean any data (records), irrespective of form and characteristics, contained and processed in information and telecommunications devices, systems and networks;

(m) "Critical information infrastructure" shall mean an assemblage of critical information infrastructure facilities and telecommunications networks used to interconnect critical information infrastructure facilities;

(n) “Critical infrastructure facilities” shall mean information systems and information and communications networks of public authorities and information systems and automated process control systems operating in the defence, healthcare, education, transport, communications, energy, banking and finance sectors, nuclear and other important areas of the life of the State and society;

(o) “service provider” shall mean:

(i) any public or private entity that provides to users of its services the ability to communicate by means of ICT, and

(ii) any other entity that processes or stores electronic information on behalf of an entity referred to in (i) above or the users of the services provided by such entity;

(p) “Traffic data” shall mean any electronic information (excluding the contents of the transferred data) relating to the transfer of data by means of ICT and indicating, in particular, the origin, destination, route, time, date, size, duration and type of the underlying network service;

(q) “ICT device” shall mean an assemblage (grouping) of hardware components used/designed for automatic processing, storage and transfer of electronic information;

(r) “Electronic evidence” shall mean any evidentiary information stored or transmitted in digital form (on an electronic medium).

The term “substantial harm” shall be determined in accordance with the domestic law of the requested State Party.

Chapter II
Criminalization, criminal proceedings and law enforcement

Section 1
Establishment of liability

Article 5
Establishment of liability

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law at minimum the acts envisaged in articles 6, 7, 9–12, 14–17, 19, 20, 22–26 and 28 of this Convention, while applying such criminal and other penalties, including imprisonment, that take into account the level of public danger posed by a given act and the magnitude of the damage caused.

Article 6
Unlawful access to digital information

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law intentional unlawful access to digital information that has resulted in its destruction, blocking, modification or copying.

Article 7
Unlawful interception

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional interception of digital information, carried out without appropriate authorization and/or in violation of established rules, including that involving the use of technical means to intercept traffic data and data processed by means of ICT that are not intended for public use.

Article 8
Unlawful interference with digital information

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law intentional unlawful interference with digital information by damaging, deleting, altering, blocking, modifying or copying it.

Article 9
Disruption of information and communications networks

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law an intentional and unlawful act, aimed at disrupting information and communication networks, that causes or threatens to cause serious consequences.

Article 10
Creation, utilization and distribution of malicious software

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional creation, including adaptation, use and distribution of malicious software intended for the unauthorized destruction, blocking, modification, copying or dissemination of digital information, or neutralization of its security features, except for lawful research.

2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the creation or utilization of a botnet for the purpose of committing any of the acts envisaged in articles 6–12 and 14 of this Convention.

Article 11
Unlawful interference with critical information infrastructure

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional creation, distribution and/or use of software or other digital information knowingly designed to interfere unlawfully with critical information infrastructure, including software or other digital information for the destruction, blocking, modification, copying of information contained therein, or for the neutralization of security features.

2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the violation of the rules of operation of media designed for storage, processing and transfer of protected digital information contained in critical information infrastructure or information systems or information and communication networks that belong to critical information infrastructure, or the violation of the rules of access to them, if such violation damages the critical information infrastructure.

Article 12
Unauthorized access to personal data

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law unauthorized access to personal data in order to destroy, modify, copy or share it.

Article 13
Illegal trafficking in devices

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the illegal manufacture, sale, purchase for use, import, export or other form of transfer for use of devices designed or adapted primarily for the purpose of committing any of the offences established under articles 6–12 of this Convention. The provisions of this article shall apply when the manufacture, sale, purchase for use, import, export or other form of transfer for use of devices is related, for example, to an authorized trial or to protection of a computer system.

Article 14
ICT-related theft

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the theft of property or the illegal acquisition of rights over it, including by means of fraud through destruction, blocking, modification or copying of digital information or other interference with ICT operations.

2. Each State party may reserve the right to consider ICT-related theft of property or the illegitimate acquisition of rights over it, including by means of fraud, to be an aggravating circumstance when such theft is committed in such forms as are defined in its domestic law.

Article 15

ICT-related offences connected with the production and distribution of materials or objects with pornographic images of minors

1. Each State party shall also adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the following acts, committed intentionally and unlawfully:

(a) producing child pornography for the purpose of its distribution through information and communication networks, including the Internet;

(b) offering or making available child pornography through information and communication networks, including the Internet;

(c) using information and communication networks, including the Internet, to distribute, transmit, publicly display, or advertise child pornography;

(d) using ICT to procure child pornography oneself or for another person;

(e) possessing child pornography in a computer system or on electronic digital data storage devices.

2. For the purposes of paragraph 1, 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.

For the purposes of this article, 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.

Article 16
Encouragement of or coercion to suicide

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the encouragement of or coercion to suicide, including of minors, through psychological or other pressure over information and telecommunication networks, including the Internet.

Article 17
Offences related to the involvement of minors in the commission of illegal acts that endanger their life or health

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the use of ICT to involve minors in the commission of life-threatening illegal acts, except for acts provided for in article 16 of this Convention.

Article 18
The creation and use of digital information to mislead the user

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the intentional illegal creation and use of digital information capable of being mistaken for information already known and trusted by a user, causing substantial harm.

2. Each State party may reserve the right to consider such acts to be criminal if they are committed in conjunction with other offences under the domestic law of that State party or involve the wilful intent to commit such offences.

Article 19
Incitement to subversive or armed activity

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law calls issued by means of ICT for subversive or armed activities directed towards the violent overthrow of the government of another State.

Article 20
Terrorism-related offences

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law calls issued by means of ICT for the commission of terrorist activities, for incitement, recruitment, or other involvement in terrorist activities, for advocacy and justification of terrorism, or for collection or provision of funds for its financing.

Article 21
Extremism-related offences

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic, or religious hatred or enmity, advocacy and justification of such actions, or to provide access to such materials, by means of ICT.

2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law humiliation by means of ICT of a person or group of people on account of their race, ethnicity, language, origin or religious affiliation.

Article 22
Offences related to the distribution of narcotic drugs and psychotropic substances

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law intentional illicit trafficking in narcotic drugs and psychotropic substances, as well as materials required for their manufacture, by means of ICT.

Article 23
Offences related to arms trafficking

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law intentional illicit trafficking in arms, ammunition, explosive devices and explosive substances by means of ICT.

Article 24
Rehabilitation of Nazism, justification of genocide or crimes against peace and humanity

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional dissemination by means of ICT of materials that deny, approve or justify actions that amount to genocide or crimes against peace and humanity, established by the Judgment of the International Military Tribunal formed under the London Agreement of 8 August 1945.

Article 25
Illegal distribution of counterfeit medicines and medical products

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional illegal distribution of counterfeit medicines and medical products by means of ICT.

Article 26
Use of ICT to commit acts established as offences under international law

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the use of ICT for the purpose of committing an act constituting an offence under any of the international agreements listed in the Annex to this Convention.

2. When depositing its instrument of ratification, acceptance, approval or accession, a State that is not a party to an agreement listed in the Annex to this Convention may declare that, in the application of this Convention to that State party, the agreement shall be deemed not to be included in the aforementioned annex. The declaration shall cease to have effect as soon as the treaty enters into force for the State party, which shall notify the depositary of that fact.

3. When a State party ceases to be a party to an agreement listed in the Annex to this Convention, it may make a declaration with respect to that agreement (agreements), as provided for in paragraph 2 above.

Article 27
Infringement of copyright and related rights by means of ICT

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the infringement of copyright and related rights, as defined by the legislation of that State party, when such acts are intentionally committed by means of ICT, including

the illegal use of software for copyrighted computer systems or databases and appropriation of authorship.

Article 28
Aiding, preparing and attempting the commission of an offence

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the preparation for and attempt at the commission of any offence established as such under this Convention.

2. Each State party shall consider taking such legislative and other measures as are necessary to establish as offences under its domestic law the manufacture or adaptation of instruments and other means of crime by a person, the solicitation of accomplices, conspiring to commit an offence or any other intentional creation of conditions for the commission of an offence established as such under this Convention, in instances in which the offence is not committed because of reasons beyond that person's control.

3. Each State party shall adopt such legislative and other measures as are necessary under its domestic law to establish liability, along with the actual perpetrators of an offence established as such under this Convention, of the organizer, abettor or aider who participate in its commission, as well as strengthen the liability for collective crimes, including organized groups and criminal associations.

Article 29
Other illegal acts

This Convention shall not preclude a State party from establishing as an offence any other illegal act committed intentionally by means of ICT that causes substantial harm.

Article 30
Liability of legal persons

1. Each State party shall adopt such legislative and other legal measures as are necessary to ensure that legal persons can be held liable for a criminal offence or other illegal act established as such under this Convention, when such an offence or act was committed for their benefit by any natural person, acting either individually or as part of an entity of the respective legal person, and holding a leadership position within it by virtue of:

(a) a power of attorney of the legal person;

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

(c) authority to exercise control within the legal person.

2. In addition to the cases provided for in paragraph 1 of this article, each State 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 or other illegal

act established as such under 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 State party, the liability of a legal person may be criminal, civil or administrative. The State party shall ensure that legal persons held liable are subject to effective, proportionate and dissuasive sanctions, including monetary sanctions.

4. Such liability of legal persons shall be without prejudice to the liability of the natural persons who have committed the offence or other illegal act.

Section 2
Criminal proceedings and law enforcement

Article 31
Scope of procedural provisions

1. Each State party shall adopt such legislative and other measures as are necessary to establish the powers and procedures envisaged in this section for the purposes of preventing, detecting, suppressing, exposing and prosecuting offences and other illegal acts, and conducting judicial proceedings relating to such offences and acts.

2. Except as otherwise provided in article 33 of this Convention, each State party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences and other illegal acts established in accordance with articles 6–29 of this Convention;

(b) Other criminal offences and other illegal acts committed by means of ICT;

(c) The collection of evidence, including electronic evidence, relating to the commission of criminal offences and other illegal acts.

3. (a) Each State party may make a reservation to the effect that it retains the right to apply the measures referred to in article 38 of this Convention only to criminal offences or categories of criminal offences specified in the reservation, provided that the range of such criminal offences or categories of criminal offences is not more restricted than the range of criminal offences to which it applies the measures referred to in the provisions of article 33 of this Convention. Each State party shall consider restricting the application of such a reservation to enable the broadest application of the measures provided for under article 38 of this Convention;

(b) If a State party, owing to limitations in its domestic legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 33 and 38 of this Convention to the information being transmitted within an information system of a service provider, and that system

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

(ii) does not employ an information and telecommunications network and is not connected with other information systems,

that State party may reserve the right not to apply those measures to such information transmission.

Article 32
Conditions and safeguards

1. Each State 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 legislation, which shall ensure the adequate protection of human rights and freedoms, including rights arising from the obligations that the State party has undertaken under the International Covenant on Civil and Political Rights of 16 December 1966 and other applicable international human rights instruments.

2. In view of the nature of the powers and procedures concerned, such conditions and safeguards shall include, inter alia, judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such powers or procedures.

3. To the extent that it is consistent with the public interest, in particular as regards the administration of justice, the State party shall consider the impact of the powers and procedures provided for in this section on the rights, responsibility and legitimate interests of third parties.

Article 33
Collection of information transmitted by means of ICT

1. In order to counter the offences covered by this Convention and established as such under its domestic legislation, each State party shall adopt such legislative and other measures as are necessary to empower its competent authorities to:

(a) Collect or record, through the application of technical means, in the territory of that State party, information transmitted by means of ICT; and

(b) Oblige a service provider, to the extent that it possesses the technical capacity to do so:

(i) to collect or record, through the application of technical means in the territory of that State party, electronic information which includes data on content and is transmitted by means of ICT; or

(ii) to cooperate with and assist the competent authorities of that State party in real time collection or recording of electronic information which includes data on content and is transmitted by means of ICT in the territory of that State party.

2. Where a State party, owing to the long-established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of electronic information which includes data on content and is transmitted by means of ICT in its territory through the application of technical means in that territory.

3. Each State party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the exercise 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 the provisions of articles 31 and 32 of this Convention.

Article 34
Expedited preservation of accumulated electronic information

1. Each State party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to give adequate orders or instructions or similarly ensure the expeditious preservation of specified electronic information, including traffic data, in particular where there are grounds to believe that the data is particularly vulnerable to deletion, copying or modification, including due to expiry of the retention period provided for by its domestic legislation or by the provider's terms of service.

2. If a State party gives effect to the provisions of paragraph 1 of this article by means of an order to a person (including legal persons) to preserve specified stored information in the person's possession or control, the State party shall adopt such legislative and other legal measures as may be necessary to oblige that person to preserve such information and maintain its integrity for such period of time as in necessary, but no longer than the period determined by the domestic legislation of that State party, to enable the competent authorities to seek disclosure of the data. A State party may provide for such an order to be subsequently renewed.

3. Each State party shall also adopt such legislative and other measures as may be necessary to oblige the person who is tasked with preserving the information to keep confidential the undertaking of such procedures for the period of time provided for by its domestic legislation.

4. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

Article 35
Expedited preservation and partial disclosure of traffic data

1. Each State party shall adopt, in respect of traffic data that is to be preserved under the provisions of article 34 of this Convention, such legislative and other measures as may be necessary to:

(a) Ensure that such expeditious preservation of traffic data is possible, regardless of how many service providers were involved in the transmission of such information; and

(b) Ensure the expeditious disclosure to the competent authorities of that State party of a sufficient amount of traffic data to enable the respective State party to identify the service providers and the path through which the indicated information was transmitted.

2. The powers and procedures referred to in this article shall be subject to the provisions of articles 31 and 32 of this Convention.

Article 36
Production order

1. For the purposes set out in article 31, paragraph 1, of this Convention, each State 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 provide specified electronic information in that person's possession or control;

(b) A service provider offering its services in the territory of that State party to submit subscriber information in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

3. For the purposes of this article, the term "subscriber information" shall mean any information held by a service provider relating to subscribers to its services other than traffic data or content data, on the basis of which it is possible to establish:

(a) The type of information and communications service used, the technical provisions taken thereto and the period of service;

(b) The subscriber's identity, postal or other addresses, telephone and other access numbers, including IP addresses and billing and payment information, available in the service agreement or arrangement;

(c) Information relating to the location of information and telecommunications equipment that has a bearing on the service agreement or arrangement.

Article 37
Search and seizure of information stored or processed electronically

1. Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seek access in the territory or under the jurisdiction of that State party to:

(a) ICT devices and information stored therein; and

(b) Information storage media in which the electronic information sought may be stored.

2. Each State party shall adopt such legislative and other measures as may be necessary to ensure that where its competent authorities, conducting a search pursuant to the provisions of paragraph 1 (a) of this article, have grounds to believe that the information sought is stored on another ICT device in the territory of that State party, such authorities shall be able to expeditiously conduct the search to obtain access to that other ICT device or the data contained therein.

3. Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize electronic information in the territory or under the jurisdiction of the State party, or similarly secure such information. These measures shall include the provision of the following powers:

(a) To seize an ICT device used to store information or to secure it in another way;

(b) To make and retain copies of such information in electronic and digital form;

(c) To maintain the integrity of the relevant stored information;

(d) To remove from the ICT device information stored or processed electronically.

4. Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order, under the procedure established by its domestic legislation, any person who has special knowledge about the functioning of the information system in question, information and telecommunications network, or their component parts, or measures applied to protect the information therein, to provide the necessary information and/or assistance in undertaking measures referred to in paragraphs 1–3 of this article.

5. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

Article 38
Real-time collection of traffic data

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

(a) Collect or record, employing technical means for this purpose, the traffic data associated with ICT use in the territory of that State party; and

(b) Oblige service providers, to the extent that they possess the technical capacity to do so:

(i) to collect or record traffic data in the territory of that State party, employing technical means for this purpose; or

(ii) to cooperate with and assist the competent authorities of that State party in collecting or recording in real time the traffic data associated with specified information in the territory of that State party.

2. Where a State party, owing to the long-standing principles of its domestic legal system, cannot adopt the measures provided for in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of the traffic data in its territory through the application of technical means in that territory.

3. Each State party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the exercise 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 the provisions of articles 31 and 32 of this Convention.

Article 39
Jurisdiction

1. Each State party shall take all measures necessary to establish jurisdiction over criminal offences and other illegal acts established as such under this Convention, when they are committed:

(a) In the territory of that State party; or

(b) On board a vessel flying the flag of that State party when the offence was committed, or onboard an aircraft registered under the law of that State party at that time.

2. Subject to article 3 of this Convention, a State party may also establish its jurisdiction over any such offence and other illegal act when:

(a) The offence is committed against a national of that State party, a stateless person permanently residing in its territory, a legal person established or having a permanent representation in its territory, a State or government facility, including the premises of a diplomatic mission or consular office of that State party; or

(b) The offence is committed by a national of that State party or a stateless person whose habitual residence is in its territory; or

(c) The offence is committed against that State party; or

(d) The offence is committed wholly or partly outside the territory of that State party but its effects in the territory of that State party constitute an offence or result in the commission of an offence.

3. For the purposes of article 47 of this Convention, each State party shall take all measures necessary to establish its jurisdiction over the offences established as such under this Convention when the alleged offender is present in its territory and the State party does not extradite such person solely on the grounds that he or she is a national of that State party or a person to which it has granted refugee status.

4. Each State party in whose territory an alleged perpetrator is present and which does not extradite such person shall, in cases provided for in paragraphs 1 and 2 of this article, without any exception and regardless of whether the offence was committed in the territory of that State party, submit the case without further delay to its competent authorities for the purpose of legal prosecution in accordance with the law of that State.

5. If a State party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified or has otherwise learned that any other States parties are investigating, prosecuting or conducting a judicial proceeding with respect to the same act, the competent authorities of those States parties shall, as appropriate, consult each other with a view to coordinating their actions.

6. Without prejudice to general international law, this Convention shall not exclude the exercise of any criminal or administrative jurisdiction established by a State party in accordance with its domestic law.

Chapter III
Measures to prevent and combat offences and other illegal acts in cyberspace

Article 40
Policies and practices to prevent and combat offences and other illegal acts relating to ICT use

1. Each State party shall, in accordance with the fundamental principles of its legal system, develop and implement or pursue an effective and coordinated policy to combat offences and other illegal acts relating to ICT use.

2. Each State party shall endeavour to establish and promote effective practices to prevent offences and other illegal acts relating to ICT use.

3. The States parties shall, as appropriate and in accordance with the fundamental principles of their legal systems, collaborate with each other and relevant international and regional organizations in promoting and developing the measures referred to in this article.

Article 41
Bodies responsible for preventing and combating offences and other illegal acts relating to ICT use

1. Each State party shall take all legislative and other legal measures necessary to designate authorities responsible for activity to prevent and combat offences and other illegal acts relating to ICT use, and establish procedures for the interactions between such authorities.

2. Each State party shall inform the Secretary-General of the United Nations of the name and address of the authority/authorities who may assist other States parties in developing and implementing specific measures to prevent offences and other illegal acts relating to ICT use.

Article 42
Private sector

1. Each State party shall take measures, in accordance with the fundamental principles of its domestic law, to prevent offences and other illegal acts relating to ICT use in the private sector, enhance information security standards in the private sector and, where appropriate, impose and apply effective, proportionate and dissuasive civil, administrative and criminal sanctions for failure to comply with such measures.

2. Measures aimed at attaining these goals may include, inter alia:

(a) Promoting cooperation between law enforcement agencies of the State party and relevant private entities of that State party;

(b) Promoting the development of standards and procedures to ensure information security;

(c) Promoting training programmes for law enforcement, investigative, judicial and prosecutorial officials relating to ICT use.

Article 43
Principles and codes of conduct for private providers of information and telecommunications services

1. Each private provider (or grouping of such providers) of information and telecommunications services located in the territory of a State party shall take appropriate measures, within its power and in accordance with the law of the State where it is located, to support the establishment and implementation of principles and standards for the use of international cyberspace, based on respect for human rights as guaranteed by fundamental instruments of the United Nations.

2. Measures aimed at attaining these goals may include, inter alia:

(a) Cooperation among private providers of information and telecommunications services or groupings of such providers;

(b) Cooperation in developing principles and standards for creating an enabling environment for the construction of civilized society as an integral part of international cyberspace.

Article 44
Raising public awareness of cybercrime prevention

1. Each State party shall take appropriate measures, within its power and in accordance with the fundamental principles of its domestic law, to promote the active involvement of public organizations in the prevention of offences and other illegal acts relating to ICT use, and to raise public awareness of those offences, their causes and seriousness, as well as of the threats that they pose. This involvement should be backed by the following measures:

(a) The provision of effective public access to information;

(b) The conduct of public consciousness-raising activities to promote zero tolerance of offences and other illegal acts relating to ICT use, as well as with the aim of disseminating best practices;

(c) The conduct of public education training programmes on ICT security.

2. Each State party shall take appropriate measures to ensure that the public is aware of the relevant bodies responsible for combating offences and other illegal acts relating to ICT use referred to in this Convention, and provide access to such bodies for the reporting of any incidents that may be considered offences and other illegal acts in accordance with this Convention.

Article 45
Measures for protecting witnesses

Each State party shall consider adopting such legislative measures as may be necessary to provide effective protection for the following:

(a) Persons who, in good faith and on reasonable grounds, provide information relating to illegal acts covered by articles 6–28 of this Convention or otherwise cooperate with investigating or judicial authorities;

(b) Witnesses who give testimony concerning illegal acts covered by articles 6–28 of this Convention, as well as victims;

(c) Where appropriate, family members of the persons referred to in subparagraphs (a) and (b) of this article.