A Proposal for a United Nations Convention on Cybercrime

By

Stein Schjolberg
Chief judge (ret.)
(January 2, 2023)

Introduction

Recognizing that regulation on how criminal activities committed in cyberspace could be dealt with through legislation in an internationally compatible manner.
Noting that The Council of Europe Convention on Cybercrime was adopted on November 8. 2001 and opened for signature in Budapest November 23, 2001. The Convention is ratified by 68 States (December 2022), including 24 States outside Europe. A 2nd Additional Protocol to the Convention on Cybercrime was approved at a meeting on June 7-9. 2017, and the proposal was adopted by the Council of Europe on November 17, 2021.
Recognizing that the United Nations Congresses on Crime Prevention and Criminal Justice has been organized every fifth year since 2005.
Recalling that the GCA Chairman Report (2008) in International Telecommunication Union (ITU) considered the Council of Europe's *Convention on Cybercrime* as an example of legal measures realized as a regional initiative, and that countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal systems and practice.
Noting that more than 125 countries have signed and/or ratified cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity at the international level.
Recalling that the United Nations Office on Drugs and Crime (UNODC) has since 2011 organized Intergovernmental Expert Groups for developing proposals on national and international legal responses to cybercrime.
Noting that the United Nations General Assembly Resolution of December 27. 2019 on Countering the use of information and communications technologies for criminal purposes was adopted by a recorded vote of 79 in favor and 60 against, with 30 abstentions.
Recognizing that searching for a global common ground on legal measures in a United Nations regulation should be a priority.
Noting that States should discuss a common ground on legal measures in a United Nations regulation that should be based on the Council of Europe Cybercrime Convention, and additional Articles. It should also be based on *The Second Additional Protocol to the Convention on Cybercrime* (2021).

Recognizing that the principle of State sovereignty applies in cyberspace.

Based on The Ad Hoc Committee proposal of November 7, 2022,
but updated Article 2, updated Article 4, updated Article 6-12, 17, 18, with Articles in the Budapest Convention, and
New Article 56: International law enforcement

Chapter I
General provisions

Article 1. Statement of purpose
The purposes of this Convention are to:
(a) Promote and strengthen measures to prevent and combat cybercrime, while protecting users of information and communications technologies from such crime;
(b) Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and
(c) Provide practical measures to enhance technical assistance among States Parties, build the capacity of national authorities to prevent and combat cybercrime, in particular for the benefit of developing countries, and strengthen and promote the exchange of information, specialized knowledge, experiences and good practice.

Article 2. Use of terms
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 any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and 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.

Article 3. Scope of application
1. This Convention shall apply, in accordance with its terms, to the prevention, detection, investigation and prosecution of cybercrime, including the freezing, seizure, confiscation and return of the proceeds of offences established in accordance with this Convention.
2. This Convention shall also apply to the collecting, obtaining, preserving and sharing of evidence in electronic form of offences set forth in this Convention.
3. For the purposes of implementing this Convention, it shall not be necessary, except as otherwise stated herein, for the offences set forth in it to result in damage or harm to persons, including legal persons, property and the State

Article 4. Protection of sovereignty

1.The principle of State sovereignty applies in cyberspace.
A State enjoys sovereign authority, with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.
A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.

2. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.
3. Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

Article 5. Respect for human rights

1. States Parties shall ensure that the implementation of their obligations under this Convention is in accordance with applicable international human rights law.

2. States Parties shall make efforts to mainstream a gender perspective and to take into consideration the special circumstances and needs of vulnerable groups, in particular women, children and the elderly, in measures undertaken to prevent and combat cybercrime.

Chapter II
Criminalization

Article 6. 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 7. 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 8. 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 9. 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 10. 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 Articles 2.2 through 2.5,
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 2.2 through 2.5; 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 2.2 through 2.5. 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 2.2 through 2.5 of this Convention, such as for the authorized 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.

Article 11. 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 of 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 12. 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.

Article 13. Information and communications technology-related theft
1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, the theft of property or the illegal acquisition of rights over it, through the destruction, blocking, modification or copying of computer data or other interference with information and communications technologies operations.
2. Each State Party may consider information and communications technology-related theft of property, or the illegitimate acquisition of rights over it, to be an aggravating circumstance of the offence of theft as defined in the domestic law of the State Party.

Article 14. Illicit use of electronic payment instruments
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, the following acts:
(a) The forging, fabrication or installation of any device or materials that facilitate the forgery or imitation of any electronic payment instrument by any means;
(b) The appropriation, use or provision to others of the data of any payment instrument, or the facilitation of the obtainment of such data by others;
(c) The use of an a computer system to gain unauthorized access to the data pertaining to any payment instrument;
(d) The knowing acceptance of a forged payment instrument.

Article 15. Violation of personal information
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and unlawfully, the accessing, sale, provision or otherwise making available of any material containing personal information about a person, including information related to a person's bank account, with the intent of obtaining a financial benefit, and subsequent disclosure, without the consent of the person concerned, of such material to any other person.

Article 16. Identity-related offences
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:
(a) The obtaining, receiving or distribution of passwords or credentials for access to a computer system without right; and
(b) The fraudulent or dishonest use of the electronic signature, password or any other unique identification feature of any other person.

Article 17. 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 willfully, 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.

Article 18. Offences related to combating online child sexual abuse

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.

Article 19. Facilitation of child abuse material through a computer system or an information and communications technology system.

1. Each State 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 lawful excuse, creating, developing, altering, maintaining, controlling, moderating, assisting, making available, advertising or promoting a computer system or an information and communications technology system for the purposes of facilitating child abuse material as identified in article 18 of this Convention.

2. For the purposes of paragraph 1, the term "facilitating child abuse" shall include any of the conduct outlined in paragraph 1 carried out for the purposes of allowing persons to access or produce "child abuse material" or to transmit, distribute, offer or make available such material to themselves or other persons.

Article 20. Grooming or procuring of a child for sexual purposes through a computer system or an information and communications technology system

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, grooming, agreeing, making arrangement with, propositioning, procuring, soliciting, coercing or luring a child, for the

purpose of facilitating, encouraging, offering or soliciting unlawful sexual conduct of or with a child or a person believed to be a child, or causing it to witness or otherwise engage in sexual activities through a computer system or an information and communications technology system.
2. For the purpose of paragraph 1 “child” also includes a person who is believed to be under 18 years of age.
3. No criminal liability is established if a person has taken reasonable steps to ascertain that the person is not a child.

Article 21. Cyberstalking of a child
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the use of a computer system or information and communications technology system to compile, transmit, publish, reproduce, buy, sell, receive, exchange or disseminate the name, telephone number, electronic mail address, residence address, picture, physical description, characteristics or any other identifying information on a child in furtherance of an effort to arrange a meeting with the child for the purpose of engaging in sexual intercourse, sexually explicit conduct or unlawful sexual activity.

Article 22. Involvement of minors in the commission of illegal acts
Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence the use of a computer system or an information and communications technology system to involve minors in the commission of illegal acts that endanger their lives or their physical or mental health, except for acts provided for in article 23 of this Convention.

Article 23. Encouragement of or coercion to suicide
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences the encouragement of or coercion to suicide, including of children, through psychological or other forms of pressure applied through the use of a computer system or an information and communications technology system.

Article 24. Sexual extortion
1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the threat to distribute or transmit, by electronic means, an intimate image of another person, with the specific intent to:
(a) Harass, threaten, coerce, intimidate or exert any undue influence on the person, especially in order to obtain a financial or other material benefit, including to compel the victim to engage in unwanted sexual activity; or
(b) Obtain a financial or other material benefit, including to compel the victim to engage in unwanted sexual activity.
2. For the purpose of paragraph 1, “intimate image” means a visual recording of a person made by any means including a photographic, film or video recording:
(a) In which the person is nude, is exposing their genital organs, anal region or breasts, or is engaged in explicit sexual activity;
(b) In respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
(c) In respect of which the person continued to have a reasonable expectation of privacy at the time the offence was committed.

Article 25. Non-consensual dissemination of intimate images

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and unlawfully, the publishing, distributing, transmitting, selling, making available, or advertising of an intimate image of a person by means of a computer system or an information and communications technology system, with the intent to cause serious emotional distress knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct.
2. For the purpose of paragraph 1, "intimate image" means a visual recording of a person made by any means, including a photographic, film or video recording:
(a) In which the person is nude, is exposing their genital organs, anal region or breasts, or is engaged in explicit sexual activity;
(b) In respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
(c) In respect of which the person continued to have a reasonable expectation of privacy at the time the offence was committed.
3. No criminal liability is established if the non-consensual sharing has a legitimate purpose.
4. A child cannot consent to the posting of an intimate image of which he or she is the subject.

Article 26. Incitement to subversive or armed activities

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

Article 27. Extremism-related offences

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences the distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic or religious hatred, the advocacy and justification of such acts and the provision of access to such materials by means of a computer system or information and communications technology system.

Article 28. Denial, approval, justification or rehabilitation 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 information and communications technology-related intentional dissemination of materials that deny, approve, justify or rehabilitate 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 29. Terrorism-related offences

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed by means of information and communications technologies, the commission of terrorist acts, the incitement, recruitment or other involvement in terrorist activities, the advocacy and justification of terrorism or the collection or provision of funds for its financing, training for terrorist acts, the facilitation of communication between terrorist organizations and their members, including the establishment, publication or use of a website or the provision of logistical support for

perpetrators of terrorist acts, the dissemination of methods for making explosives employed in particular in terrorist acts, and the spreading of strife, sedition, hatred or racism.

Article 30. Offences related to the distribution of narcotic drugs and psychotropic substances

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, illicit trafficking in narcotic drugs and psychotropic substances and materials necessary for their manufacture through the use of an information and communications technology system or a computer system.

Article 31. Offences related to arms trafficking

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, illicit trafficking in arms, ammunition, explosive devices and explosive substances by means of information and communications technologies.

Article 32. Illegal distribution of counterfeit medicines and medical products

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, the intentional and illegal distribution of counterfeit medicines and medical products by means of information and communication technologies.

Article 33. Money-laundering

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a) (i) The conversion or transfer of property, including virtual currencies, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her actions;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement, or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

(b) Subject to the basic concepts of its legal system:

(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

2. For purposes of implementing or applying paragraph 1 of this article:

(a) Each State Party shall seek to apply paragraph 1 of this article to the widest range of predicate offences;

(b) Each State Party shall include as predicate offences relevant offences established in accordance with this Convention. In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in such list a comprehensive range of offences associated with cybercrime;

(c) For the purposes of subparagraph (b), predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only where the relevant conduct is a criminal offence under the domestic law of the State where it

is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article, had it been committed there;
(d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;
(e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence.

Article 34. Obstruction of justice
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:
(a) The use of physical force, threats or intimidation or the promise, offering or giving of an undue advantage to induce false testimony or to interfere in the giving of testimony or the production of evidence in a proceeding in relation to the commission of offences covered by this Convention;
(b) The use of physical force, threats or intimidation to interfere with the exercise of official duties by a justice or law enforcement official in relation to the commission of offences covered by this Convention. Nothing in this subparagraph shall prejudice the rights of States Parties to have legislation that protects other categories of public officials.

Article 35. Liability of legal persons
1. Each State Party shall adopt such legislative and other measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for a criminal offence established in 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, on the basis of:
    1. (a) A power of representation of the legal person;
    2. (b) An authority to take decisions on behalf of the legal person;
    3. (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 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 established in accordance with this Convention for the benefit of that legal person by a natural person acting under its express or implied authority.
3. Subject to the legal principles of the State Party, the liability of legal persons 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 offences.
5. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.
6. Legal persons shall be protected from liability for an act done or omitted to be done in good faith:
(a) In the performance or intended performance of a duty imposed by or under this convention; or
(b) In the exercise or intended exercise of a function or power conferred by or under this Convention.

Article 36. Participation and attempt

1.Each State Party shall adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, the participation in any capacity, such as an accomplice, assistant, instigator, abettor or conspirator, in an offence established in accordance with this Convention, or the organization or directing of other persons to commit such an offence.

2. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, any attempt to commit an offence established in accordance with this Convention.

3. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the preparation for an offence established in accordance with this Convention.

4. Each State Party shall adopt such legislative and other measures as may be necessary to strengthen the liability for collective crimes, including those perpetrated by organized criminal groups.

5. Each State Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 37. Knowledge, intent and purpose as elements of an offence

Knowledge, intent or purpose required as an element of an offence established in accordance with this Convention may be inferred from objective factual circumstances.

Article 38. Statute of limitations

Each State Party shall, where appropriate, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence established in accordance with this Convention and establish a longer statute of limitations period or provide for the suspension of the statute of limitations where the alleged offender has evaded the administration of justice.

Article 39. Prosecution, adjudication and sanctions

1. Each State Party shall make the commission of an offence established in accordance with this Convention liable to sanctions that take into account the gravity of that offence.

2. Each State Party may impose an aggravation of penalty for offences established in accordance with this Convention, including but not limited to cases in which the commission of offences:

1. (a) Affects critical infrastructure;
2. (b) Results in the obtaining of confidential government information;
3. (c) Causes harm, including physical or psychological trauma, to individuals.

3. Each State Party shall take such measures as may be necessary to establish or maintain, in accordance with its legal system and constitutional principles, an appropriate balance between any immunities or jurisdictional privileges accorded to its public officials for the performance of their functions and the possibility, when necessary, of effectively investigating, prosecuting and adjudicating offences established in accordance with this Convention.

4. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences established in accordance with this Convention are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.

5. Each State Party shall ensure that any person prosecuted for offences established in accordance with this Convention enjoys all rights and guarantees in conformity with the law

of the State in the territory of which that person is present and with relevant and applicable provisions of international human rights law, including the right to a fair trial and the rights of defence.
6. In the case of offences established in accordance with this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.
7. Each State Party shall take into account the gravity of the offences concerned when considering the eventuality of early release or parole of persons convicted of such offences.
8. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.
9. States Parties shall endeavour to promote the reintegration into society of persons convicted of offences established in accordance with this Convention.
6. In the case of offences established in accordance with this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.
7. Each State Party shall take into account the gravity of the offences concerned when considering the eventuality of early release or parole of persons convicted of such offences.
8. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.
9. States Parties shall endeavour to promote the reintegration into society of persons convicted of offences established in accordance with this Convention.

Chapter III
Procedural measures and law enforcement

Article 40. Jurisdiction
1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when:
    1. (a) The offence is committed in the territory of that State Party; or
    2. (b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.
2. Subject to article 4 of this Convention, a State Party may also establish its jurisdiction over any such offence when:
(a) The offence is committed against a national or a legal person of that State Party; or
(b) The offence is committed by a national or legal person of that State Party or a stateless person who has his or her habitual residence in its territory; or

(c) The offence is committed outside its territory with a view to the commission of an offence established in accordance with this Convention within its territory;
(d) The offence is committed against the State Party;
(e) The offence involves the computer data of the State Party's nationals, irrespective of the place of its physical storage, processing or screening.
3. For the purposes of the article on extradition of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.
4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.
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 conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.
6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Article 41. Scope of procedural measures
1. Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings.
2. Except as provided otherwise in article 48 of this Convention, 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 this Convention;
(b) Other criminal offences committed by means of a computer system; and
(c) The collection of evidence in electronic form of offences set forth in this Convention.
3. (a) Each State Party may reserve the right to apply the measures in article 47 of this Convention 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 criminal offences to which the State Party applies the measures referred to in article 48. Each State Party shall consider restricting such a reservation to enable the broadest application of measures on real-time collection of traffic data.
(b) Where a State Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply measures on real-time collection of traffic data and on interception of content data 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 State Party may reserve the right not to apply these measures to such communications. Each State Party shall consider restricting such a reservation to enable the broadest application of measures on real-time collection of traffic data and on interception of content data.

Article 42. Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter 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 and fundamental freedoms arising from its obligations under applicable international human rights law, and which shall incorporate the principles of proportionality, necessity and legality and the protection of privacy and personal data.
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 article upon the rights, responsibilities and legitimate interests of third parties.

Article 43. Expedited preservation of stored computer data

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 obtain or ensure 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 deletion, copying, loss 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. Where a State Party gives effect to paragraph 1 above by means of an order to a person, including legal persons, to preserve specified stored computer data in the person's possession or control, the State 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 State Party may provide for such an order to be subsequently renewed.
3. Each State 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 legislation.
4. The powers and procedures referred to in this article shall be established in accordance with articles 41 and 42 of this Convention.

Article 44. Expedited preservation and partial disclosure of traffic data

1. Each State Party shall adopt, in respect of traffic data that are to be preserved under the provisions of the article on expedited preservation of stored computer data, 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 State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication or indicated information was transmitted.
2. The powers and procedures referred to in this article shall be subject to articles 41 and 42.

Article 45. Production order

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to order:
(a) A person in its territory to submit specified computer data in that person's possession or control that 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 State 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 41 and 42.
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 it is possible to establish:
(a) The type of information and communications technology service used, the technical provisions applied thereto and the period of service;
(b) The subscriber's identity, postal or geographic addresses, telephone and other access numbers, and billing and payment information, available on the basis of the service agreement or arrangement;
(c) Information relating to the location of information and communications equipment available on the basis of the service agreement or arrangement.

Article 46. Search and seizure of stored computer data

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to search or similarly access in the territory or under the jurisdiction of that State Party:
(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.
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 reasonable grounds to believe that the computer data sought is stored in another computer system in the territory of that State Party, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously conduct the search to obtain access to that other computer system 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 or similarly secure computer data in its territory or under its own jurisdiction accessed in accordance with paragraphs 1 or 2, or similarly secure such information. These measures shall include the power to:
(a) Seize or secure in another way a computer system or part of it, or a medium used to store computer data;
(b) Make and retain copies of such computer data;
(c) Maintain the integrity of the relevant stored computer data;
(d) Render inaccessible or remove the computer data in the accessed computer system.
4. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has special knowledge about the functioning of the computer system in question, the information and telecommunications network, or their component parts, 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 to 3 of this article.
5. The powers and procedures referred to in this article shall be subject to articles 41 and 42.

Article 47. 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, where there is reasonable belief that a criminal offence was committed or is being committed, to undertake the following actions with respect to traffic data associated with specified communications in its territory transmitted by means of a computer system in the territory of that State party:
(a) Collect or record, in real time, through the application of technical means in the territory of that State Party; and
(b) Compel a service provider, within its existing technical capability:
(i) To collect or record, in real time, through the application of technical means in the territory of that State Party; or
(ii) To cooperate and assist the competent authorities in the collection or recording, in real time, of such data associated with specified information in the territory of that State Party.
2. Where a State Party, owing to the fundamental 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 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 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 41 and 42.

Article 48. Interception of content data
1. Each State 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 undertake the following actions with respect to content data of specified communications in its territory transmitted by means of a computer system:
(a) Collect or record, in real time, through the application of technical means in the territory of that State Party; and
(b) Compel a service provider, within its existing technical capability:
(i) To collect or record, in real time, through the application of technical means in the territory of that State Party; or
(ii) To cooperate and assist the competent authorities in the collection or recording of such data in real time.
2. Where a State Party, owing to the fundamental 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 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 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 41 and 42.

Article 49. Admission of electronic evidence
Electronic evidence derived or extracted from devices, equipment, electronic media, information systems, computer programs or any information and communications technologies shall have the probative value of material forensic evidence in criminal procedure when such evidence meets the technical conditions under the laws of the States Parties concerned.

Article 50. Freezing, seizure and confiscation of the proceeds of crime
1. Each State Party shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:
(a) Proceeds of crime derived from offences established in accordance with this Convention or property the value of which corresponds to that of such proceeds;
(b) Property, equipment or other instrumentalities used in or destined for use in offences established in accordance with this Convention.
2. Each State Party shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.
3. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.
4. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.
5. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.
6. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

Article 51. Establishment of criminal record
Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as, and for the purpose that, it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence established in accordance with this Convention.

Article 52. Protection of witnesses
1. Each State Party shall take appropriate measures within its means to provide effective protection from potential retaliation or intimidation for witnesses who give testimony or, in good faith and on reasonable grounds, provide information concerning offences established in accordance with this Convention or otherwise cooperate with investigative or judicial authorities and, as appropriate, for their relatives and other persons close to them.
2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:
(a) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where appropriate, non-disclosure or

limitations on the disclosure of information concerning the identity and whereabouts of such persons;
(b) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means.
3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.
4. The provisions of this article shall also apply to victims insofar as they are witnesses.

Article 53. Assistance to and protection of victims
1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences established in accordance with this Convention, in particular in cases of threat of retaliation or intimidation.
2. Each State Party shall establish appropriate procedures to provide access to compensation, and restitution, for victims of offences established in accordance with this Convention.
3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

Article 54. Compensation for damage
Each State Party shall take such measures as may be necessary, in accordance with principles of its domestic law, to ensure that entities or persons who have suffered damage as a result of cybercrime have the right to initiate legal proceedings against those responsible for that damage in order to obtain compensation.

Article 55. Measures to enhance cooperation with law enforcement authorities
1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in offences established in accordance with this Convention:
(a) To supply information useful to competent authorities for investigative and evidentiary purposes on such matters as:
(i) The identity, nature, composition, structure, location or activities of persons participating in offences established in accordance with this Convention;
(ii) Links, including international links, with other persons participating in offences established in accordance with this Convention;
(iii) Other offences that persons participating in offences established in accordance with this Convention have committed or may commit;
(b) To provide factual, concrete help to competent authorities that may contribute to depriving persons participating in offences established in accordance with this Convention of their resources or of the proceeds of crime.
2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating the punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence established in accordance with this Convention.
3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence established in accordance with this Convention.
4. Protection of such persons shall be as provided for in the article on protection of witnesses of this Convention.
5. Where a person referred to in paragraph 1 of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States

Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

Article 56. International law enforcement

1.INTERPOL shall have the global responsibility for the coordination of all regional and national law enforcement organizations on cybercrime investigations, and all global investigations against cybercriminals.
2. INTERPOL shall provide operational investigative support to police across all its member countries, for an efficient cross-border cooperation, such as on forensics, analysis, training, and networking of the cybercrime investigations.
3. INTERPOL shall provide an I-24/7 network as the technical platform that enables police in one country to immediately identify experts in other countries and obtain real-time assistance in cybercrime investigations and evidence collections.