United Nations A/AC.291/9/Add.1

General Assembly

Distr.: General
21 April 2022
English
Original: Arabic/English/French/
Russian/Spanish

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
Second session
Vienna, 30 May–10 June 2022

Compilation of proposals and contributions submitted by Member States on the provisions on criminalization, the general provisions and the provisions on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes

Addendum

V.22-02329 (E) 110522 120522

Contents

III. General provisions

Angola

[Original: English]
[8 April 2022]

General provisions

Definitions: cybercrime, electronic evidence, interception, computer system, computer data, metadata, traffic data, service providers, computer program, electronic communications network, critical infrastructure, topography, semiconductor product, cyberspace sovereignty.

For the elaboration of the concepts suggested here, it is possible to resort to the regional and international legal instruments mentioned above.[1]

Australia

[Original: English]
[13 April 2022]

General provisions should include:

- A statement of purpose that is clearly focused on combating cybercrime
- Scope of application that is targeted and clearly defines
- Agreed definitions, which should be discussed and agreed only after the substantive articles of the Convention are settled.

The nature of cyberspace, as distinguished from physical space, adds complexities to the application and interpretation of international law rules and principles, including the principle of State sovereignty, and to the application of territorial jurisdiction. Australia suggests that discussions on how these legal issues might be addressed in the Convention continue in parallel to the elaboration of substantive provisions.

Brazil

[Original: English]
[8 April 2022]

Chapter I
General provisions

Article 1
Purpose[2]

The purpose of this Convention is to prevent and counter cybercrimes by establishing:

(a) Conduct which Parties shall punish as offences in their territories;

(b) Procedural powers for the timely action of national authorities; and

(c) International cooperation measures.

[1] Note by the Secretariat: this reference is to those instruments included under a different subheading: African Union Convention on Cyber Security and Protection of Personal Data, Council of Europe Convention on Cybercrime, United Nations Convention against Transnational Organized Crime and United Nations Convention against Corruption.

[2] *Source*: original proposal submitted by Brazil.

Article 2
Scope of application[3]

1. This Convention shall apply to:

(a) The prevention, detection, disruption, investigation, prosecution and adjudication of cybercrimes;

(b) The implementation of measures to mitigate the consequences of cybercrimes; and

(c) Any relevant international cooperation to prevent and counter cybercrimes.

2. For the purpose of implementing this Convention, it shall not be necessary for the offences to result in property damage, except as otherwise provided herein.

Article 3
Use of terms[4]

For the purposes of this Convention:

(a) "Affected person" means any person, service provider or other entity who has been, or is likely to be, affected by the grant of any order in this part;

(b) "Computer data" includes any representation of data or information that have been, or are capable of being, stored, transmitted or otherwise processed in a computer system. They include subscriber traffic, and content data;

(c) "Computer system" means any device or group of interconnected or related devices, one or more of which, pursuant to a program or other software, stores, transmits or otherwise processes computer data;

(d) "Content data" means any computer data stored by a service provider or any other information other than traffic or subscriber data, such as text, voice, videos, images and sound, or the communication content of a communication;

(e) "Electronic communications network" means transmission systems, whether or not based on a permanent infrastructure or centralized administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed and mobile networks, and electricity cable systems, to the extent that they are used for the purpose of transmitting signals, irrespective of the type of information conveyed;

(f) "Electronic evidence" means any data or information generated, stored, transmitted or otherwise processed in electronic form that may be used to prove or disprove a fact in legal proceedings;

(g) "Electronic surveillance" means:

(i) The monitoring, interception, copying or manipulation of messages, data or signals that have been stored or transmitted, or are in the process of being transmitted, by electronic means; or

(ii) The monitoring or recording of activities by electronic means;

[3] Proposal by China and Russia, with changes made by Brazil.
[4] Expert group meeting to update the United Nations Office on Drugs and Crime Model Law on Mutual Legal Assistance in Criminal Matters (process ongoing on 9 March 2022), with minor changes made by Brazil.

(h) “Service provider” means:

(i) Any person, or public or private entity, that provides to users of its service the ability to communicate by means of a computer system, or otherwise facilitates communication over an electronic communications network; or

(ii) Any other person, or public or private entity, that stores or otherwise processes computer data on behalf of such service or users of such service;

(i) “Subscriber data” means any computer data, collected in the normal course of business by a service provider, pertaining to the name, date of birth, postal or geographical address, billing and payment data, device identifiers, telephone number or email address, or any other information, such as the Internet Protocol address used at the time when an account was created, which can serve to identify the subscriber or customer, as well as the type of service provided and the duration of the contract with the service provider, other than traffic or content data;

(j) “Traffic data” means any computer data collected in the normal course of business by a service provider, related to:

(i) The type of service provided and its duration where it concerns technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of the service, excluding passwords or other authentication means used instead of a password that are provided by a user, or created at the request of a user; or

(ii) The commencement and termination of a user access session to a service, such as the date and time of use, or the log-in to, and log-off from the service; or

(iii) Communications metadata as processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content, including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment processed in the context of providing communications services, and the date, time, duration and type of communication.

Burundi

[Original: French]
[8 April 2022]

Chapter I. Definitions

For the purposes of this Convention:

(a) “Unlawful access” means intentional access, without right, to the whole or any part of an electronic communication network, information system or terminal equipment;

(b) “Encryption” means any technique that transforms digital data into an unintelligible format by using cryptological means;

(c) “Cryptology” means the science of protecting and securing information;

(d) “Cybercrime” means any illegal act committed by means of a computer system or network or any other physical network connected or related to an information system;

(e) “Cyberspace” means a body of digitized data constituting a universe of information and a communication environment linked to the worldwide interconnection of automated digital data processing equipment;

(f) “Cybersecurity” means a set of technical, organizational, legal, financial, human and procedural measures for prevention, protection and deterrence, and other actions enabling those objectives to be achieved;

(g) “Electronic communication” means the emission, transmission or reception of signs, signals, text, images, sounds or video recordings by electromagnetic, optical or any other means;

(h) “Personal data” shall mean any information of any kind, regardless of the medium on which it is stored, including sound and image, relating to a natural person directly or indirectly identified or identifiable by reference to an identification number or to one or more factors specific to the physical, physiological, genetic, mental, cultural, social or economic identity of that person;

(i) “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;

(j) “Electromagnetic” means the result of the coupled vibration of an electric field and a magnetic field that is variable in time;

(k) “Service provider” means a natural or legal person that provides one or more services to users of a telecommunication system;

(l) “Information” means any element of knowledge that can be represented with the aid of devices in order to be used, preserved, processed or communicated. Information may be expressed in written, visual, audio, digital or other forms;

(m) “Critical infrastructure” means infrastructure that is essential to services vital for public safety, economic stability, national security and international stability and for the sustainability and restoration of critical cyberspace. The critical infrastructure facilities of the State consist of services relating to public health, internal and external security, defence, finance and transport that are connected to Internet networks;

(n) “Unlawful interception” means access without right or authorization to data on an electronic communications network, in an information system or in terminal equipment;

(o) “International gateway” is a generic name for a device that connects two different types of computer networks, for example a local network and the Internet;

(p) “Means of electronic payment” refers to means by which the holder is able to make electronic payment transactions online;

(q) “Phishing/fishing” means a form of fraud committed by email that consists in assuming the identity of a known and recognized company in an email with the aim of compelling the recipients to change or update their bank details on Internet pages imitating those of the company whose image has been used for the purposes of the fraud;

(r) “Child pornography” means any visual depiction, including any photograph, film, video or image, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where:

(i) The production of such visual depiction involves a minor;

(ii) Such visual depiction is a digital image, computer image or computer-generated image in which a minor is engaging in sexually explicit conduct, or where images of the sexual parts of a minor are produced or used for primarily sexual purposes and exploited with or without the child’s knowledge;

(iii) Such visual depiction has been created, adapted or modified to give the impression of a minor engaging in sexually explicit conduct;

(s) “Service providers” means mobile operators, Internet service providers and infrastructure operators;

(t) “Computer program” means a set of instructions executed by the computer to achieve the intended result;

(u) “Racism and xenophobia in information and communications technology” means any written material, any image or any other representation of ideas or theories that advocates, promotes or incites hatred, discrimination or violence against any individual or group of individuals on the basis of race, colour, descent, national or ethnic origin or religion;

(v) “Spamming” means the non-targeted sending of commercial messages in large numbers by email, with the intention of committing theft, to individuals who have not given their authorization to the sender to receive such messages;

(w) “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;

(x) “ICT” means information and communications technology.

Canada[5]

[Original: English]
[9 April 2022]

General provisions

Purpose

The purpose of this Convention is to promote cooperation in the prevention, investigation and prosecution of cybercrime more effectively.

Scope of application

This Convention shall apply, except as otherwise stated and subject to appropriate safeguards:

(a) To promote and strengthen legislative and other measures to prevent, investigate and prosecute cybercrime and serious offences that are frequently committed through the use of computer systems as established in the Convention;

(b) To promote, facilitate and support international cooperation and assistance in relation to the prevention, investigation and prosecution of offences established in this Convention;

(c) To promote, facilitate and support efficient and effective mutual legal assistance in relation to electronic evidence pertaining to the offences established in this Convention and any other criminal offences; and

(d) To promote, facilitate and support technical assistance in the prevention of and fight against cybercrime.

Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the provisions of this Convention are subject to conditions and safeguards provided for under its domestic law, which shall provide for the full protection of human rights and liberties, including rights arising pursuant to obligations under the International Covenant on Civil and Political Rights and other applicable international human rights instruments, and which shall incorporate the principles of the rule of law, legality, necessity and proportionality.

[5] Note by the Secretariat: Canada also submitted a list of definitions, available at www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

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 the power or procedure.

3. Each State Party shall implement measures to improve understanding of the linkages between gender and cybercrime, including the ways in which cybercrime can affect women and men differently. The measures shall aim to promote gender equality and the empowerment of women, including by mainstreaming it into relevant legislation, policy development, research, projects and programmes, as appropriate and in accordance with the fundamental principles of domestic law.

4. The measures set forth in this Convention shall be interpreted and applied in a way that does not interfere with freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of choice, and applicable rights concerning respect for privacy and data protection. The interpretation and application of those measures shall be consistent with internationally recognized principles of non-discrimination.

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, participation in any capacity such as an accomplice, assistant or instigator in an offence established in accordance with this Convention.

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

Corporate liability

1. Each State Party shall adopt the necessary legislative and other measures, consistent with its legal principles, to establish the liability of legal persons for participation in the commission of the offences established in the Convention.

2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.

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

4. 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.

Colombia

[Original: Spanish]
[9 April 2022]

General provisions

The States parties shall, in preventing and combating cybercrime in all its aspects, promote and ensure full respect for the rights of women and girls while also paying special attention to gender issues, in particular gender-based violence, including violence against women and girls.

The States parties shall, in preventing and combating cybercrime in all its manifestations, promote and ensure respect for human rights and fundamental freedoms. All the provisions of this convention or instrument shall be interpreted and applied in a manner consistent with the relevant international human rights obligations.

Definitions

In accordance with the consensus established during the first round of negotiations with respect to the need to agree on technologically neutral terminology and definitions, and in line with the comments made by the Council of Europe team for the Budapest Convention, the definitions set out in both the Budapest Convention and its Second Protocol are relevant, sufficient and adaptable to technological evolution and may accordingly be proposed to the Ad Hoc Committee.

Thus, the definitions to be proposed are as follows:

(a) Computer system: “any device or a group of interconnected [...] devices [...] which, pursuant to a program, performs automatic processing of data”;

(b) Computer data: “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: “any public or private entity that provides to users of its services 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: “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”;

(e) Central authority: “the authority or authorities designated under a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned, or, in the absence thereof, the authority or authorities designated by a Party […] responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution”;

(f) Competent authority: “a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorize or undertake the execution of measures [...] for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings”;

(g) Emergency: “situation in which there is a significant and imminent risk to the life or safety of any natural person”;

(h) Personal data: “information relating to an identified or identifiable natural person”;

(i) Transferring party: “the Party transmitting the data in response to a request or as part of a joint investigation team, or [...] a Party in whose territory a transmitting service provider or entity providing domain name registration services is located”;

(j) Subscriber information: “any information [...] that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: [...] the type of communication service used, the technical provisions taken thereto and the period of service [...], the subscriber’s identity, postal or geographical address, telephone [...], billing and payment information [...] any other information on the site of the installation of communication equipment”.

Egypt

[Original: Arabic]
[8 April 2022]

Chapter I. General provisions

It is proposed that this chapter cover the aims of the convention, terms used, protection of sovereignty and scope of application, as follows:

Article 1. Aims

This Convention aims to strengthen cooperation among States Members of the United Nations to counter the use of information and communications technologies for criminal purposes. It seeks to suppress actions that would threaten the integrity and confidentiality of information and communications technologies, criminalize the misuse of information and communications technologies for illegal purposes, facilitate the investigation and prosecution of perpetrators, and implement measures to eliminate the consequences of such offences. These measures include suspending transactions relating to assets obtained from the commission of any illegal act set forth in the Convention and confiscating and returning the proceeds thereof. For this purpose, the Convention provides for powers sufficient to effectively counter information and communications technology-related offences by establishing international cooperation arrangements to facilitate the detection and investigation of such offences, the prosecution of perpetrators and the extradition of offenders.

Article 2. Terms

The following terms, as used in this Convention, shall have the meanings as indicated below:

(a) Information technology: any physical or non-corporeal means, or group of interconnected or unconnected means, used to store, arrange, organize, retrieve, process, develop and exchange information according to the orders and instructions stored therein, including all inputs and outputs associated therewith, by wire or wirelessly, in a system or network;

(b) Service provider: any natural or legal person, public or private, that provides subscribers with services to communicate via information technology or that processes or stores information on behalf of a communication service or its users;

(c) Data: all such information as may be stored, processed, generated and transmitted by information technology, such as numbers, letters, symbols and the like;

(d) Information system: a set of programmes and tools designed to process and manage data and information;

(e) Information network: two or more information systems that are linked to obtain and exchange information;

(f) Site: a place where information is made available on an information network through a specific address;

(g) Capture: the viewing or obtaining of data or information;

(h) Site administrator: any person who is responsible for: organizing, managing, monitoring or maintaining one or more sites on an information network, including access rights for different users on the site; the site design; generating and organizing pages or content on the site; or the site;

(i) Private account: a set of information relating to a natural or legal person that grants that person the exclusive right to access or use the services available through a site or information system;

(j) Email: A means of exchanging electronic messages at a specific address between more than one natural or legal person via an information network or other electronic means of interconnection, computers and the like;

(k) Interception: the viewing or obtaining of data or information for the purpose of eavesdropping on, disabling, storing, copying, recording, modifying the content of, misusing, rerouting or redirecting the data or information for illegal purposes;

(l) Penetration: access to an information system, computer, information network and the like that is unauthorized, or in violation of the provisions of the relevant licence, or illegal;

(m) Content: any data that, by themselves or combined with other data or information, lead to the formation of information or the identification of a trend, direction, concept or meaning or reference to other data;

(n) Digital evidence: any electronic evidentiary information that is stored on or transmitted, extracted or obtained from computers, information networks and the like and that can be collected and analysed using special technological devices, software or applications;

(o) Traffic (traffic data): data that are produced by an information system and that show a communication's origin, destination, sender, addressee, route, time, date, size and duration and the type of service.

Article 3. Protection of sovereignty

1. The States parties shall fulfil their obligations under this Convention in accordance with their domestic laws or constitutional principles in a manner consistent with the principles of the sovereign equality of States and non-interference in the internal affairs of other States.

2. This Convention shall not permit a State party to exercise, in the territory of another State, the jurisdiction and functions that are assigned exclusively to the authorities of that other State under its domestic law.

Article 4. Scope of application

1. Except as otherwise provided, this Convention shall apply to the suppression of the offences set forth herein.

2. For the purposes of implementing this Convention, it shall not be necessary for the offences or other illegal acts set forth herein to result in material damage, except as otherwise provided herein.

3. Each State party shall consider limiting its reservation to allow for the broad application of the aforesaid measures.

El Salvador

[Original: Spanish]
[12 April 2022]

Terminology

In the opinion of our Government, there are a number of existing definitions that should be incorporated into the document, and those definitions should be worded in such a way that the translations into the six official languages of the United Nations convey the correct concepts without there being any doubt as to the concept to which reference is being made. Accordingly, it is proposed that the Ad Hoc Committee consider the definitions already established in instruments with which the Member States are familiar, such as the Budapest Convention and the United Nations Convention against Transnational Organized Crime, as a starting point for the drafting of definitions.

In particular, we believe that definitions of the following terms should be added:

(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 an action;

(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.

A definition of "material with child abuse content" rather than "child pornography" should be added, the key words being producing, reproducing, distributing, publishing, importing, exporting, offering, financing, selling, marketing, disseminating and possessing such content, and that definition should include the participation of a person who appears to be a minor in sexually explicit acts or realistic images of a minor participating in sexually explicit acts; it should also cover not only the depiction of children in sexually explicit acts but also those acts that show children and adolescents in the nude.

European Union and its member States

[Original: English]
[6 April 2022]

Chapter I. General provisions

Article 1
Statement of purpose

While ensuring a high level of protection of human rights and fundamental freedoms, the purposes of this Convention are:

(a) To promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively;

(b) To promote and facilitate international cooperation;

(c) To ensure a high level of protection of victims' rights; and

(d) To support capacity-building and technical assistance in the fight against cybercrime.

Article 2
Use of terms

For the purpose of this Convention:

(a) "Central authority" shall mean the authority or authorities designated for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution;

(b) "Cybercrime" shall mean, for the purpose of this Convention, the conduct as defined in articles 5 to 10 of this Convention;

(c) "Competent authority" shall mean a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorize or

undertake the execution of measures under this Convention with respect to specific criminal investigations or proceedings;

(d) “Computer system” shall mean any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data;

(e) “Computer data” shall mean any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function;

(f) “Personal data” shall mean information relating to an identified or identifiable natural person;

(g) “Regional economic integration organization” shall mean an organization constituted by sovereign States of a given region, to which its member States have transferred competence in respect of matters governed by this Convention and which has been duly authorized, in accordance with its internal procedures, to sign, ratify, accept, approve or accede to it; references to “States Parties” under this Convention shall apply to such organizations within the limits of their competence;

(h) “Service provider” shall mean:

(i) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(ii) Any other entity that processes or stores computer data on behalf of such communication service or users of such service;

(i) “Subscriber data” shall mean any information contained in the form of computer data or any other form that are held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

(i) The type of communication service used, the technical provisions taken thereto and the period of service;

(ii) The subscriber’s identity, postal or geographical address, telephone and other access number, and billing and payment information, available on the basis of the service agreement or arrangement;

(iii) Any other information on the communication equipment and the site of its installation, available on the basis of the service agreement or arrangement;

(j) “Traffic data” shall mean 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, data, size, duration or type of underlying service;

(k) “Without right” shall mean conduct referred to in articles 5 to 10 of this Convention that is not authorized by the owner or by another rights holder of the computer system or of part of it, or not permitted under domestic law.

Article 3
Scope of application

This Convention shall apply, except as otherwise stated herein, to:

(a) The prevention, investigation and prosecution of criminal offences established in accordance with articles 5 to 10 of this Convention;

(b) The collection of evidence in electronic form of a criminal offence established in accordance with articles 5 to 10 of this Convention on the basis of the measures set out in chapter III of this Convention;

(c) The provision and conduct of technical assistance and capacity-building on matters covered by this Convention.

Article 4
Effects of the Convention

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

2. With respect to States Parties that are members of a regional economic integration organization, those States Parties may, in their mutual relations, apply the rules of that regional economic integration organization governing the matters dealt with in this Convention.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party under international law, in particular human rights law.

Ghana

[Original: English]
[12 April 2022]

Chapter I
General provisions

Article 1
Statement of purpose

The purpose of this Convention is to promote and facilitate international cooperation as well as strengthen measures to prevent and counter the use of information and communications technologies for criminal purposes.

Article 2
Use of terms

For the purpose 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) "Content data" means the communication content of the communication, that is, the meaning or purport of the communication or the message or information being conveyed by the communication other than traffic data;

(d) "Child" means a person under 18 years of age. A Party may, however, require a lower age limit, which shall be not less than 16 years;

(e) "Critical information infrastructure" means a computer or computer system identified by a Member State in its domestic legislation as essential for national security or the economic and social well-being of citizens;

(f) “Prohibited intimate image and visual recording” includes:

(i) Moving or still image that depicts:

a. The person engaged in an intimate sexual activity that is not ordinarily done in public; or

b. The genital or anal region of a person, when the genital or anal region is bare or covered only by underwear; and

(ii) An image that has been altered to appear to show any of the things mentioned in paragraph (*i*) even if the thing has been digitally obscured, if the person is depicted in a sexual way;

(g) “Service provider” means:

(i) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(ii) Any other entity that processes or stores computer data on behalf of such communication service or users of such service;

(h) “Subscriber” means a customer or a user of an electronic communications network, electronic communications service or broadcasting service;

(i) “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 the services of a service provider other than traffic or content data and by which may be established:

(i) The type of communication service used, the technical provision taken in respect of the communication service and the period of service;

(ii) The identity, postal or geographical address, telephone and other access number of the subscriber, billing and payment information available on the basis of the service agreement or arrangement; and

(iii) Any other information on the site of the installation of a communication equipment, available on the basis of the service agreement or arrangement;

(j) “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 origin, destination, route, time, date, size or duration of the communication or the type of underlying service.

Article 3
Scope of application

This Convention shall apply, in accordance with its terms, to:

(a) The prevention, investigation and prosecution of offences established in accordance with articles 5 through 20;

(b) The collection of evidence in electronic form of a criminal offence;

(c) The provision and conduct of technical assistance and capacity-building on matters covered by this Convention;

(d) The freezing, seizure, confiscation and return of the proceeds of offences established in accordance with this Convention.

Article 4
Protection of sovereignty

1. Member States 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 domestic affairs of other States.

2. Nothing in this Convention entitles a Member State 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.

Iran (Islamic Republic of)

[Original: English]
[8 April 2022]

1. General provisions

Despite the exceptional opportunities presented by information and communications technologies for the development of nations, criminals are exponentially misusing such technologies to carry out illicit activities and realize illegitimate purposes. The modi operandi of such criminals are becoming increasingly diversified and sophisticated and the compounded nature of such offences is substantially evolving. Crimes committed via the use of information and communications technology often transcend geographical boundaries, turning them into an unprecedented pressing challenge for Member States to overcome. As such, a strengthened collective response and cooperation at the international level within a sound international legal framework is more than necessary.

The raison d'être for the establishment of the Ad Hoc Committee pursuant to General Assembly resolution 74/247 was to respond to this urgent need and to elaborate an international legal instrument that supports effective measures at various levels in fighting the use of information and communications technology for criminal purposes. To this end, the general provisions of the convention should stipulate the purposes of the convention and define its purview. As an established practice and given the underlying importance of compliance with the fundamental principles of international law in preventing and combating crimes committed via the use of information and communications technology, a substantive section should also be dedicated to such principles under the general provisions. Defining the terminologies used in the convention under a specific section is essential to ensure a common understanding of important terms and ultimately of the provisions of the convention.

1.1 Objectives of the convention

In view of the above, the Islamic Republic of Iran highlights that the convention should aim to strengthen, support and facilitate international cooperation in preventing and combating the use of information and communications technology for criminal purposes, including in asset recovery, to strengthen national responses to such crimes and to assist States parties, in particular, developing countries, in fighting these crimes, inter alia, through economic development, provision of technical assistance and transfer of technology. In this relation, the challenges and barriers such as unilateral sanctions and underdevelopment that undermine the ability of States to effectively fight the use of information and communications technology for criminal purposes should be addressed in a technical context.

Due regard should also be had for the responsibility of service providers and other similar entities in cooperating with judicial and law enforcement authorities so as to ensure effective measures in preventing and combating the use of information and communications technology for criminal purposes.

Whereas a common understanding of the criminal phenomena and its evolving forms is of utmost importance in effectively responding to crimes committed via information and communications technology, the convention should also promote and facilitate the exchange of information, expertise, specialized knowledge, experiences and good practices.

Such objectives will be well realized by adopting an approach that cherishes a shared future in cyberspace for all Member States with equal opportunities and without discrimination.

1.2. Scope of the convention

The convention should have within its purview crimes that are dependent on information and communications technology, such as crimes against the confidentiality and integrity of information and communications technology systems and data and crimes against information and communications technology infrastructure, as well as those enabled by such technologies, for example, insults to religious values, incitement to violence, encouragement to commit homicide, distribution of criminal and obscene content and child sexual exploitation. Nevertheless, crimes enabled by information and communications technology may require a case-by-case approach that considers different factors surrounding various forms of crimes and possible differences in the elements of crime necessary to establish as offences. Where appropriate, further elements may also be needed to define the ambits of the convention based on the severity or penalties of offences and taking into account whether the offences in question have been perpetrated in more than one State.

1.3 Protection of sovereignty

The Islamic Republic of Iran reaffirms that specific sections on protection of sovereignty should be included in the general provisions to ensure that efforts and measures in preventing and combating the use of information and communications technology for criminal purposes are consistent and in compliance with the fundamental principles of international law and the principles set forth in the Charter of the United Nations, in particular, sovereignty equality, territorial integrity of States and non-intervention. This is an established practice in the elaboration of conventions in the field of preventing and combating crimes; as a case in point, the term “protection of sovereignty” has been utilized in conventions such as the United Nations Convention against Corruption.

The Islamic Republic of Iran remains circumspect regarding attempts that are at variance with this established practice of the international community and aim to negate and ignore the essential role of conformity with such principles in fighting crimes.

Japan

[Original: English]
[8 April 2022]

2. General provisions

2.1 Statement of purpose

We support the three objectives outlined in the Chair’s proposal at the first session of the Ad Hoc Committee: (a) to promote and strengthen measures to prevent and combat cybercrime; (b) to promote, facilitate and strengthen international cooperation; and (c) to provide practical tools to enhance technical assistance and build the capacity of national authorities.

2.2 Use of terms

From the viewpoint of creating a convention that will be effectively utilized for a long period of time, the terms used in this convention need to be clearly defined in a technology-neutral manner. For example, it would be inappropriate to establish definitions for technologies that are constantly changing, such as “botnet”.

Therefore, definitional provisions should be established in as general and clear a manner as possible and to the extent necessary, while referring to existing international instruments such as the United Nations Convention against Transnational Organized Crime. We believe that this perspective applies equally to discussions on other parts of this convention, such as provisions on criminalization.

2.3 Scope of application

2.3.1. The scope of the application of this convention should be clearly stated based on the provisions of the United Nations Convention against Transnational Organized Crime and United Nations Convention against Corruption.

2.3.2. Cybersecurity and Internet governance should not be addressed in this convention. For example, the following measures would have a chilling effect on legitimate economic activity and would impede the development of technology, and would go beyond the mandate of the Ad Hoc Committee:

- Setting security standards under this convention
- Imposing obligations on legal persons and individuals to comply with such standards or imposing penalties for violation of such standards or
- Holding legal persons, their representatives or software creators who unintentionally engage in cybercrimes committed by other actors without awareness accountable.

Mexico

[Original: English]
[13 April 2022]

General provisions

In order to prevent possible omissions and lack of compliance with the implementation of other future legally binding instruments, and according to precedent international and regional treaties, Mexico supports the inclusion of general references as initial provisions instead of very exhaustive and detailed ones.

Regarding sovereignty, and following the example of the United Nations Framework Convention on Climate Change, Mexico recommends including from the preamble a general reference to reaffirm sovereignty, as follows: “Reaffirming the principle of sovereignty of States in international cooperation to countering the use of information and communication technologies for criminal purposes”.

Mexico also recommends including a preambular paragraph reaffirming the Charter of the United Nations, the applicability of international law and the Universal Declaration of Human Rights and other human rights obligations, as follows: “Reaffirming the purposes and principles of the Charter of the United Nations, international law, the Universal Declaration of Human Rights and other relevant instruments on human rights”.

It is also recommended that a general provision is included on the importance of States taking appropriate measures to protect people and in particular vulnerable groups: “Decided to take actions of prevention, response, mitigation, investigation and prosecution to effectively protect people and in particular vulnerable groups from the use of information and communication technologies for criminal purposes.”

As stated in this previous proposal, for the Government of Mexico it will be key to take into account in the convention measures of prevention, response, mitigation, investigation and prosecution.

During the process of negotiation of the convention it will be important to recognize the relevance of previous international legally binding instruments, and in particular the United Nations Convention against Transnational Organized Crime, by

bringing to the table concrete experiences that could be used to make international cooperation against cybercrimes more efficient. A related call to promote United Nations system-wide coherence must be included as a general provision.

Also in the preamble, Mexico recommends including explicit recognition of the opportunities and benefits brought by information and communications technologies to make clear that they are not per se used by criminal and for illicit purposes: "Recognizing that information, telecommunications and digital technologies bring opportunities to enhance development, close inequality gaps and promote inclusion, well-being, justice and the exercise of human rights, and acknowledging the importance of promoting universal access to these technologies and to protecting their benefits."

In addition, Mexico shares its interest in avoiding falling into the excessive use of safeguards that might act as a constraint, contrary to the spirit of international cooperation which should lead this process.

"The purpose of this Convention is to promote bilateral and multilateral cooperation and legal assistance, including multisectorial cooperation, to prevent, respond, investigate, mitigate and prosecute the use of information and communications technologies for criminal purposes."

Mexico considers that other general provisions must be added on the following issues: defining conflict resolution procedures; establishing an implementation review mechanism; ensuring participation and collaboration of other relevant stakeholders in supporting the efforts carried out by States parties to prevent and counter the use of information and communications technologies for criminal purposes; the recognition of the public core of the Internet and the relevance of the net neutrality approach for the purposes of the convention.

New Zealand

[Original: English]
[8 April 2022]

General provisions

8. In our view, the general provisions should consist of:

- *Purpose.* Developing an effective treaty will be best served by taking a coherent, realistic and focused approach in determining our objectives. In the view of New Zealand, our purpose should be to develop a harmonized, modern and effective global framework for cooperation and coordination between States to tackle the growing threat posed by cybercrime to individuals, businesses and Governments. This includes the provision of support and technical assistance for all States to develop capacity and capability to respond to these challenges.
- *Scope of application.* Likewise, the scope of application should be targeted and clearly defined. The Chair's proposal contained in conference room paper A/AC.291/CRP.8/Rev.1 provides a good basis for determining the scope of the convention.
- *Agreed definitions.* Definitions should be precise, unambiguous, future-proof and, where possible, based on relevant existing international and regional instruments.
- A comprehensive instrument must also include a general provision that emphasizes the protection of human rights and fundamental freedoms and respect for the rule of law, taking into particular account the perspectives of women, children, indigenous peoples and vulnerable groups.

9. We have also heard from a number of States that the inclusion of a provision relating to State sovereignty is important to them. We would note that the application

of any such provision in the context of this convention must take into account some critical features that distinguish cyberspace from the physical realm. In particular: (a) cyberspace contains a virtual element that has no clear territorial link; and (b) cyberactivity may involve cyber infrastructure operating simultaneously in multiple territories and diffuse jurisdictions.

Annex II
Definitions

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

"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 to perform such a function.

"Child sexual exploitation material" shall mean any material, including in the form of images, video or live stream, that depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child for primarily sexual purposes.

"Property" shall mean assets of every kind, including digital assets, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.

Norway

[Original: English]
[8 April 2022]

General provisions

1. The convention should include strong provisions on the protection of human rights and fundamental freedoms, including the right to privacy and the protection of personal data. We must guarantee full compatibility of a future United Nations cybercrime convention with international legal obligations in this area.

2. In order to be effective, this instrument should provide the necessary safeguards, including proportionality, legality and necessity of law enforcement action.

3. The purpose should focus on international cooperation to prevent and combat cybercrime.

Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan

[Original: Russian]
[7 April 2022]

Chapter I. General provisions

Article 1. Aims

The aims of this Convention are:

(a) To promote the adoption and strengthening of measures to effectively prevent and combat information and communications technology-related crimes and other illegal acts;

(b) To prevent actions targeting the confidentiality, integrity and availability of information and communications technology, and to prevent the misuse of information and communications technology, 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 levels and by developing arrangements for international cooperation;

(c) 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 information and communications technology-related crimes.

Article 2. Scope of application

1. 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.

2. 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 information and communications technology 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 to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography of 25 May 2000;

(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 technology” 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 they are 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, health-care, 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 information and communications technology; or

(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 information and communications technology 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 or 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.

South Africa

[Original: English]
[14 April 2022]

Chapter I. General provisions

Article 1. Statement on objectives

The objectives of the Convention shall be:

(a) To promote and strengthen measures to prevent and combat the use of information and communications technologies for criminal purposes/cybercrime, while protecting information and communications technology users from such crime;

(b) To promote and strengthen measures aimed at effectively preventing and combating crimes and other unlawful acts in the field of information and communications technologies;

(c) To promote, facilitate and support international cooperation in preventing and combating the use of information and communications technologies for criminal purposes/cybercrime;

(d) To provide practical tools to enhance technical assistance among States Parties and build the capacity of national authorities to prevent and combat the use of information and communications technologies for criminal purposes/cybercrime, and strengthen measures to promote the exchange of information, experiences and good practices.

Article 2. Use of terms

For the purposes of this Convention:

(a) ‘‘Article’’ means any:

(i) Data;

(ii) Computer program;

(iii) Computer data storage medium; or

(iv) Computer system;

which:

a. Is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;

b. May afford evidence of the commission or suspected commission; or

c. Is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission, of:

i. An offence in terms of this Convention;

ii. Any other offence brought about through the use of information and communications technologies; or

iii. An offence in a foreign State that is substantially similar to an offence contemplated in this Convention;

(b) “Child sexual abuse materials” means any image, however created, or any description or presentation, including any photograph, film, video, image, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

(i) The production of such visual depiction involves a minor;

(ii) Such visual depiction is a digital image, computer image or computer-generated image where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge; and

(iii) Such visual depiction has been created, adapted or modified to appear that a minor is engaging in sexually explicit conduct;

(c) ''Computer'' means any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes any data, computer program or computer data storage medium that are related to, connected with or used with such a device;

(d) "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;

(e) ''Computer data storage medium'' means any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system;

(f) ''Computer program'' means data representing instructions or statements that, when executed in a computer system, cause the computer system to perform a function;

(g) ''Computer system'' means:

(i) One computer; or

(ii) Two or more interconnected or related computers, which allow these interconnected or related computers to:

a. Exchange data or any other function with each other; or

b. Exchange data or any other function with another computer or a computer system;

(h) "Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

(i) "Cyber-dependent crimes" are offences that can only be committed using a computer, computer networks or other form of information and communications technology;

(j) "Cyber-enabled crimes" are crimes that do not depend on computers or networks but have been transformed in scale or form by the use of the Internet and communications technology;

(k) ''Data message'' means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form;

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

(m) "Electronic evidence" shall mean any evidentiary information stored or transmitted in digital form (on an electronic medium);

(n) "Freezing of assets" shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

(o) “Property” shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to or interest in such assets;

(p) “Proceeds of crime” shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;

(q) “Predicate offence” shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 23 of this Convention and domestic legislation of the State Party/Member State;

(r) “Seizure of assets” shall mean taking permanent control of the assets or permanent assumption of custody or control of property on the basis of an order issued by a court or other competent authority;

(s) “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, or any other entity that processes or stores computer data on behalf of such communication service or users of such service;

(t) “Traffic data” means data relating to a communication indicating the communication’s origin, destination, route, format, time, date, size, duration or type of the underlying service.

Article 3. Scope of application

This Convention shall apply, in accordance with its terms, to the prevention, investigation and prosecution of cyber-dependent and/or specific cyber-enabled crimes brought about by the use of information and communications technologies for criminal purposes and to the freezing, seizure, confiscation and return of the proceeds of offences established in accordance with this Convention.

Article 4. Protection of sovereignty

1. 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.

2. Nothing in this Convention shall entitle 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.

Switzerland

[Original: English]
[8 April 2022]

2.1. General provisions

Statement of purpose

The purposes of this Convention are:

(a) To promote and strengthen measures to [prevent/counter and combat] cybercrime efficiently and effectively;

(b) To promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against cybercrime.

Respect for and protection of human rights and fundamental freedoms

States Parties must carry out their obligations under this Convention in a manner consistent with their obligations under international human rights law.

Use of terms

"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.

"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.

"Service provider" means:

(a) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(b) Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

"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.

Scope of application

This Convention shall apply, except as otherwise stated herein, to the prevention, investigation, and prosecution of the offences established in accordance with the provisions on criminalization of this Convention.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[12 April 2022]

Chapter. General provisions

Article 1. Purpose

The purpose of this Convention is to promote international cooperation and technical assistance to prevent and combat cybercrime.

Article 2. Definitions

For the purposes of this Convention:

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

(b) "Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

(c) "Service provider" means:

(i) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(ii) Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

(d) "Traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

Article 3. Scope of application

1. This Convention shall apply, except as otherwise stated herein, to the prevention, investigation and prosecution of the offences established in this Convention.

2. This Convention may also apply, where stated herein, to the collection of evidence in electronic form of a criminal offence.

Article 4. Protection of human rights

Each Party shall ensure that the implementation of its obligations under this Convention is in accordance with international human rights law.

Additional comments

The United Kingdom believes it may also be appropriate for the general provisions chapter to address how this convention relates to, and complements, other United Nations criminal justice instruments, and to include a commitment to mainstream a gender perspective into implementing the convention's provisions.

United Republic of Tanzania

[Original: English]
[8 April 2022]

3. General provisions

The purpose of the Convention should be to promote cooperation on countering the use of information and communications technologies for criminal purposes. The cyber world is revolving and there is a wide range of terminologies used in information and communications technologies to date. It is imperative that the Convention defines terms that are universally applied in information and communications technologies to avoid ambiguities or misunderstandings.

3.1. Definition of terms

It is the view of the United Republic of Tanzania that the Convention should provide for the definition of terms in a neutral, technological manner to accommodate rapid technological changes. The terms should include the following:

(a) Access;

(b) Access provider;

(c) Caching provider;

(d) Child;

(e) Child pornography;

(f) Computer system;

(g) Computer data;

(h) Confiscation;

(i) Contraband;

(j) Cryptography;

(k) Cyberterrorism;

(l) Data;

(m) Data message;

(n) Data storage medium;

(o) Electronic data;

(p) Freezing;

(q) Hinder in relation to a computer system;

(r) Interactive message system;

(s) Interception in relation to a function of computer;

(t) Interconnection;

(u) Originator;

(v) Racist and xenophobic material;

(w) Seizure;

(x) Service provider in relation to information and communications technology;

(y) Traffic data.

3.2. Jurisdiction

The Convention should provide for legislative and such measures as may be necessary for each State party to establish its jurisdiction over the offences established under the Convention when:

(a) The offence is committed in the territory of that State party;

(b) The offence is committed on board a vessel that is flying a flag of that State party or an aircraft that is registered under the laws of that State party;

(c) The offence is directed against computer system, device or data or person located in the territory of that State party;

(d) The offence is committed by or against a national of that State party.

United States of America

[Original: English]
[8 April 2022]

Use of terms

"Child" means any individual under the age of 18.

"Child sexual abuse material" shall mean any visual depiction or live transmission of: (a) a child engaged in real or simulated sexually explicit conduct; or (b) an adult engaged in real or simulated sexuality explicit conduct with a child intentionally included in the visual depiction or live transmission. It shall not be necessary for the child to be conscious or aware of, or able to appraise the nature of, such sexually explicit conduct.[6]

"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 to perform such a function.

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

[6] Adapted from the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography, art. 2 (c).

"Confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority.[7]

"Cybercrimes" means offences established in accordance with this Convention.

"Freezing" or "seizure" shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority.[8]

"Predicate offence" shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in the criminalization of the laundering of proceeds of cybercrime article of this Convention.[9]

"Proceeds of crime" shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence.[10]

"Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.[11]

"Regional economic integration organization" shall mean an organization constituted by sovereign States of a given region, to which its member States have transferred competence in respect of matters governed by this Convention and which has been duly authorized, in accordance with its internal procedures, to sign, ratify, accept, approve or accede to it; references to "States Parties" under this Convention shall apply to such organizations within the limits of their competence.[12]

"Service provider" means: (*a*) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and (*b*) any other entity that processes or stores computer data on behalf of such a communication service or users of such service.

"Sexually explicit conduct" includes at least the following real or simulated acts: (*a*) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child; (*b*) bestiality; (*c*) masturbation; (*d*) sadistic or masochistic abuse in a sexual context; or (*e*) lascivious exhibition of the genitals or the pubic area of a child, whether clothed or nude.

"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.

Scope of application

This Convention shall apply, except as otherwise stated herein, to the prevention, investigation and prosecution of the offences established in accordance with this Convention and collecting, obtaining and sharing electronic evidence.

Protection of human rights and fundamental freedoms and the rule of law

1. States Parties shall carry out their obligations under this Convention with full respect for human rights and fundamental freedoms and the rule of law.

2. Nothing in this Convention shall be interpreted as affecting other rights and obligations of States and individuals under international law, including the Charter of the United Nations and international human rights law.

[7] Organized Crime Convention, art. 2 (g).
[8] Ibid., art. 2 (f).
[9] Ibid., art. 2 (h).
[10] Ibid., art. 2 (e).
[11] Ibid., art. 2 (d).
[12] Ibid., art. 2 (j).

3. Any person who is taken into custody or regarding whom any other measures are taken or proceedings are carried out pursuant to this Convention shall enjoy all rights and guarantees in conformity with the law of the State in the territory of which that person is present and with relevant provisions of international human rights law, including the International Covenant on Civil and Political Rights.

Protection of sovereignty[13]

1. 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.

2. Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction or performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

Venezuela (Bolivarian Republic of)

[Original: Spanish]
[13 April 2022]

4. General provisions

In this context, the general provisions of the convention must be aligned with the basic principles of public international law as an integral part of the future instrument, as enshrined in the Charter of the United Nations, including, inter alia, the recognition of sovereignty and territorial jurisdiction in accordance with the national legislation of States, which includes application of the principle of sovereignty to cyberspace, non-interference in the internal affairs of, and respect for the territorial integrity of, other States, and the peaceful settlement of disputes.

The convention should establish the principle of complementarity with other international instruments, both multilateral and regional, with regard to transnational crime, such as the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime, and compliance with responsibilities under international human rights law, including the human rights conventions.

In that regard, the Bolivarian Republic of Venezuela emphasizes that, as is the case with other international legal instruments, this instrument should not create an artificial conflict between the concepts of national sovereignty and human rights, which are intrinsically complementary.

This chapter should include definitions of key terms and expressions used in the convention.

Viet Nam

[Original: English]
[12 April 2022]

Chapter I. General provisions

1. Objectives

(a) To promote and strengthen measures to prevent and combat use of information and communications technologies for criminal purposes;

(b) To promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against the use of information and

[13] Organized Crime Convention and Convention against Corruption, art. 4.

communications technologies for criminal purposes, including asset recovery, in accordance with fundamental principles of international law and in a manner of respecting human rights.

2. Scope of application

This Convention shall apply to the prevention, investigation and prosecution of the use of information and communications technologies for criminal purposes.

3. Protection of sovereignty

(a) Member States shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality, territorial integrity of States, non-threat or use of force and non-intervention in the domestic affairs of other States;

(b) Nothing in this Convention shall allow a Member State 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 Member State by its domestic law.

4. Definitions

(a) “Cyberspace” means a network of information technology infrastructure that includes telecommunications networks, the Internet, computer networks, communication systems, information processing and control systems, and databases;

(b) “Information system” means a combination of hardware, software and databases established to serve the creation, transmission, collection, processing and storage of information in cyberspace;

(c) “Cyberattack” means the use of cyberspace, information technology or electronic devices to sabotage or interrupt the telecommunications network, the Internet, computer networks, communication systems, information processing and control systems, databases or electronic devices;

(d) “Cyberterrorism” means an act of terrorism or financing of terrorism that involves the use of cyberspace, information technology or electronic devices;

(e) “Personal information” means information associated with the identification of a natural person;

(f) “Digital data” is composed of signals, letters, numbers, images, sound or similar elements created, stored and transmitted or acquired through electronic means;

(g) “Cyberspace infrastructure” means a system of infrastructure serving creation, transmission, collection, processing and storage of information and data in cyberspace.