United Nations A/AC.291/9

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

Summary

In preparation for the second session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, the present document was prepared by the Committee Chair with the support of the secretariat. It comprises proposals received from Member States with regard to the provisions on criminalization (A/AC.291/9), the general provisions (A/AC.291/9/Add.1) and the provisions on procedural measures and law enforcement (A/AC.291/9/Add.2).

V.22-02323 (E) 170522 180522

Please recycle

Contents

I. Introduction

1. In preparation for the second session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, and in line with the road map and mode of work for the Ad Hoc Committee approved at its first session, in particular its paragraphs 3 and 4, Member States were invited to provide to the secretariat draft texts of chapters or provisions that are to be examined during the second session, in regard of the provisions on criminalization (A/AC.291/9), the general provisions (A/AC.291/9/Add.1) and the provisions on procedural measures and law enforcement (A/AC.291/9/Add.2).

2. On that basis, the Committee Chair, with the support of the secretariat, prepared the present negotiating document containing a compilation of the proposals and contributions from Member States, focused on the specific chapters to be examined during the second session. The present document therefore contains only specific drafting suggestions or general comments on the chapters on criminalization, general provisions and procedural measures and law enforcement and grouped them according to chapter, as received from Member States and translated into the six official languages of the United Nations. Unless indicated otherwise, footnotes contain text as received from Member States.

3. As mentioned above, the present document does not contain comments on other topics or explanations of specific drafting suggestions, which may be found in the original submissions, which were made available on the website of the Ad Hoc Committee as received and in their original version at the time of receipt.

4. As at 14 April 2022, 24 submissions were received by the secretariat, representing the views of 54 Member States and the European Union.

II. Criminalization

Angola

[Original: English]
[8 April 2022]

- The convention should typify and criminalize the most serious conduct of cybercrime, especially when they affect critical infrastructure, classifying them as cyberterrorism or crimes against humanity, and define priority and urgent rules of international cooperation for investigation and prosecution of cybercrime agents.
- The Convention should typify and criminalize cybercrime conducts involving cryptocurrencies and cryptoassets for the financing of terrorism and money-laundering.

Criminalization

Cyber-dependent crimes (crimes against the confidentiality, integrity and availability of computer systems and data): illegal access, illegal interception, damage to computer data, computer sabotage, computer falsity, illegal reproduction of a computer programme.

Cyber-instrumental crimes (traditional crimes committed using information and communication technologies): online scams, phishing, online economic and financial crime, online identity theft, sexual abuse and exploitation of children online, cyberbullying, cyberstalking, revenge porn, cyberterrorism.

For the construction of the concepts of these legal types of crime, it is possible to resort to the regional and international legal instruments mentioned above.[1]

Australia

[Original: English]
[13 April 2022]

Criminalization

The new convention offers the opportunity to improve international cooperation in relation to cybercrime while at the same time ensuring consistency with, and avoiding unnecessary duplication of, existing international crime conventions and other relevant instruments. Criminalization articles should be consistent with existing international instruments and avoid conflicts between such instruments. Criminalization articles should also be appropriately balanced with respect for the rule of law, human rights and fundamental freedoms.

Australia considers that the new convention offers an opportunity to increase global harmonization of cybercrime offences. This will in turn reduce safe havens for cybercriminals and enhance the ability of law enforcement to be able to combat cybercriminal activity online.

The new conventions' substantive criminal law provisions should be specific and clearly articulate the underlying criminal conduct. The convention should also give due consideration to predicate offences and ancillary liability for cyber-dependent and cyber-enabled crimes. This should include the standard extensions of criminal liability included in instruments such as the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption.

Cyber-dependant crimes

Australia considers that the new convention should include standards for the criminalization of offences directed at computer systems ("cyber-dependent crimes"). Australia proposes that the following cyber-dependant criminal offences should be included in the new convention:

- Illegal access to any part of a computer system (including computer data) without right
- Illegal interception of transmissions of computer data without right
- Illegal interference with computer data (including deletion, deterioration, alteration or suppression of computer data) without right
- Illegal interference with the functioning of a computer system or network
- Producing, supplying, distributing or obtaining malicious software for the purposes of committing another cybercrime

Cyber-enabled crimes

Almost all States' existing domestic criminal laws are adequate to capture familiar crimes, inter alia, trespass, vandalism, theft and narcotics-related and other violent crimes.

[1] Note by the secretariat: This reference is to those instruments included under the subheading "Preamble" of the submission by Angola, namely: "African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), Council of Europe Convention on Cybercrime (Budapest Convention), United Nations Convention against Transnational Organized Crime and United Nations Convention Against Corruption ".

The Convention does not need to reimagine these crimes simply because a computer system or digital technology was involved in their commission, if the use of a computer system in the commission of the offence doesn't change the character or the seriousness of the offending behaviour.

However, Australia considers that there are some "traditional" crimes whose scope, scale and ease of commission have all been drastically increased by the speed, anonymity and widespread reach that information and communications networks provide. These crimes can be described as "cyber-enabled" crimes. The Convention should address these crimes judiciously by developing a clear framework for identifying why certain crimes are so significantly altered by a "cyber element" that they require a new harmonized international standard that elevates this conduct above "traditional" crimes. The Convention does not need to create new categories of offences for every existing crime which may incorporate a "cyber element", particularly where the severity, scale, scope or ease of commission of the criminalized conduct is not significantly altered by that element.

While Australia believes that the convention should adopt a restrained approach to including any new crime category, Australia is open to hearing arguments in support of broadening the convention beyond cyber-dependent crimes to "cyber-enabled crimes".

To this end, Australia noted with appreciation the many calls to address the severe threat posed by online child sexual exploitation and abuse during the first session of the Ad Hoc Committee. Australia considers this to be an issue where countries can constructively reach consensus. In recognition of this serious criminality, Australia has separately made a proposal for offences covering online child abuse, including online grooming and livestreaming.

Australia also sees the significant increase in cyber-enabled fraud and theft, including ransomware-related extortion, as a widespread issue where States may reach consensus to criminalize this conduct for the purposes of the convention.

Criminalization of online child abuse offences

Article [A] – Child abuse material through a computer 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 [without lawful excuse][2] the following conduct:

(a) Accessing, controlling, transmitting, distributing, offering, procuring, producing or making available child abuse material through a computer system;[3] or

(b) Possessing child abuse material resulting from the conduct in subparagraph 1(a).

2. For the purposes of article [A], the term "child abuse material" shall include material that depicts or describes a child, or a representation of a child, who is implied to be, or appears to be engaging in sexual activities or in the presence of a person

[2] This caveat is included to ensure the offence does not unintentionally capture certain legitimate situations – for example, where there may be a medical requirement to access or produce material which would otherwise be captured by this provision.

[3] "Computer system" is defined to mean any device or group of interconnected or related devices, where one or more of them performs automatic processing of data pursuant to a programme. This may include input, output and storage facilities. It would also include standalone systems or one networked with other devices. Note that this term (or its definition) may be altered to ensure consistency with other provisions of the draft convention.
Self-generated material may cover both material which is purely self-generated, and also coerced or extorted self-generated material. In these contexts, the provision aims to provide a general stance of extra caution around criminalization but still leaving it to domestic legal systems to decide on their own proportionate and reasonable response.

engaging in sexual activities, any representation of the sexual parts of a child[4] for primarily sexual purposes, or a victim of torture, cruel, inhumane or degrading treatment or punishment.

Article [B] – Facilitation of child abuse material through a computer 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 [without lawful excuse],[5] creating, developing, altering, maintaining, controlling, moderating, assisting,[6] making available, advertising or promoting a computer system for the purposes of facilitating child abuse material as identified in article [A].

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

Article [C] –Grooming or procuring of a child for sexual purposes through a computer system

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, through a [computer system] grooming, making a proposal, procuring or causing a child, to meet, witness or participate in sexual activities.

Article [X] – General provisions related to the proposal

1. For the purposes of articles [A, B, C] the term "child" shall include all persons under 18 years of age. In addition, for the purposes of article [C], "child" also includes a person who is believed to be under 18 years of age.[7] For the purposes of articles [A, B, C], a State Party may, however, require a lower age limit, which shall be not less than 16 years.

2. For the purposes of articles [A, B, C], criminal liability shall apply to persons 18 years of age and above. Each State Party may at any time declare to apply such criminal liability to persons under the age of 18 years. If a State Party does declare, they shall ensure there are appropriate safeguards in their domestic law to protect the child accused, noting the impact that being subject to a criminal justice process may have on a child.

3. Where a State Party seeks to criminalize persons under the age of 18 years of age for article [A], it shall take due account of avoiding the over criminalization of children that have self-generated material captured under article [A], paragraph 2, and the need to respect their obligations under the Convention on the Rights of the Child and its Protocols.

Associated penalties

We propose that an article be included that provides for an obligation for State Parties to adopt legislative or other measures necessary to ensure that any criminal offences established under this convention are punishable by effective, proportionate and dissuasive measures, which may include deprivation of liberty.

---

[4] Terminology from Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

[5] As per footnote 2.

[6] "Assisting" may ultimately be captured by extensions of criminal responsibility general provisions. It is retained here until those provisions are considered.

[7] The addition of belief here is intended to cover situations where a person of interest or person being investigated for grooming or procuring children for sexual purposes is engaging with a law enforcement officer online in an undercover capacity.

Brazil

[Original: English]
[8 April 2022]

Chapter II
Criminalization

Article 4
Illegal access[8]

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 5
Data interference[9]

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

Article 6
System interference[10]

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 7
Illegal interception[11]

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
Computer-related fraud[12]

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,

[8] *Source*: Council of Europe Convention on Cybercrime (Budapest Convention).
[9] *Source*: Council of Europe Convention on Cybercrime.
[10] *Source*: Council of Europe Convention on Cybercrime.
[11] *Source*: Council of Europe Convention on Cybercrime.
[12] *Source*: Council of Europe Convention on Cybercrime.

(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 9
Illegal access to passwords and credentials[13]

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 procurement, obtaining or receiving of passwords or access credentials to a computer system without right.

Article 10
Misuse of devices[14]

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 4 through 9;

(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 4 through 9; and

(b) The possession of an item referred to in paragraph 1 (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in articles 4 through 9. 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 4 through 9 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[15]

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 are directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

[13] *Source*: The original proposal of Brazil.
[14] *Source*: Council of Europe Convention on Cybercrime.
[15] *Source*: Council of Europe Convention on Cybercrime.

Article 12
Offences related to child pornography[16]

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, subparagraphs (d) and (e), and 2, subparagraphs (b) and (c).

Article 13
Encouragement of or coercion to suicide[17]

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

Article 14
Infringement of copyright and related rights by means of information and communications technology[18]

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other unlawful act under its domestic law the infringement of copyright and related rights, as defined by the legislation of that State party, when such acts are intentionally committed by means of information and communications technology, including the illegal use of software for copyrighted computer systems or databases and appropriation of authorship.

[16] *Source*: Council of Europe Convention on Cybercrime.
[17] *Source*: Proposal of China and the Russian Federation.
[18] *Source*: Proposal of China and the Russian Federation.

Article 15
Attempt and aiding or abetting[19]

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with the chapter II of the Convention.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with the chapter II of the Convention.

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

Article 16
Corporate liability[20]

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

(a) A power of representation of the legal person;

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

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

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

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

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

Article 17
Sanctions and measures[21]

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with chapter II of the Convention are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with article 16 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

[19] *Source*: Council of Europe Convention on Cybercrime, with changes made by Brazil.
[20] *Source*: Council of Europe Convention on Cybercrime.
[21] *Source*: Council of Europe Convention on Cybercrime.

Burundi

[Original: French]
[8 April 2022]

Chapter II. Offences against the confidentiality, integrity and availability of computer data and systems

Section 1
Action directed against the confidentiality of computer systems

Section 2
Illegal access

The States Parties to this Convention shall establish as a criminal offence under their domestic law, when committed intentionally, the accessing of the whole or any part of a computer system without right.

Section 3
Interference with a computer system

The States Parties to this Convention shall establish as a criminal offence under their domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

Section 4
Data interference

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their 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.

Section 5
Illegal manufacture, sale, purchase, use, import, distribution or possession of a computer system and encouragement of suicide

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the manufacture, sale, purchase, use, import, distribution or possession of a computer or computer system, or the act of making computer data, programs or systems available with a view to their use or their availability to others, for the purpose of committing offences.

Section 6
Computer-related fraud

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, when committed intentionally and without right, the causing of damage to the property of another person through (a) the inputting, alteration, deletion or suppression of computer data, or (b) any form of interference with the functioning of a computer system, with fraudulent or criminal intent to obtain an undue financial benefit for the person himself or herself or for another person.

§1. Fraud in computer systems

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the use of a fraudulent scheme, by means of electronic communication, to obtain or attempt to obtain money, movable property,

bonds, deposits, instruments, pledges, receipts, releases, or the whole or any part of the property of another person.

§2. Digital identity theft

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of assuming the digital identity of another person or using one or more items of data of any kind that identify that person with a view to causing that party anxiety or harming his or her reputation, privacy or property, or that of a third party, for gain or in order to mislead other persons.

§3. Phishing

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the use of a website or the sending of an electronic message with the aid of a computer system with the intention of obtaining confidential information from the person visiting the website or from the recipient of the message in order to use that information for criminal purposes.

§4. Breach of trust in relation to computer data

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the misappropriation or dissipation of computer data entrusted to a person on the understanding that he or she will return them or use them for a specific purpose.

§5. Unlawful receiving of computer data

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the possession, in any capacity, of computer data obtained by means of an offence, in the knowledge of how the data was obtained.

§6. Extortion of computer data

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of attempting to obtain computer data by means of force, violence or coercion.

§7. Blackmail and publishing of rumours

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of making threats in writing or verbally, making revelatory or defamatory statements or extorting or attempting to extort computer data.

§8. Spamming

The States Parties to this Convention shall establish as criminal offences, without prejudice to their domestic law, the following acts:

1. The sending of unsolicited messages repeatedly or to a large number of people using a computer or computer system;

2. The use of a computer or computer system to forward a received message to multiple persons or to resend it multiple times to a person who does not need it.

Section 7
Content-related offences

§1. Offences related to child pornography

The States Parties to this Convention shall establish as criminal offences, without prejudice to their domestic law, the following conduct, when committed

intentionally and without right: producing child pornography for the purpose of its distribution through a computer system; offering or making available child pornography through a system.

Section 8
Racist or xenophobic text and images through a computer system

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of creating, downloading, disseminating or making available in any form whatsoever text, messages, photographs, drawings, videos or any other representation of ideas or theories of a racist or xenophobic nature by means of a computer system.

Section 9
Insult committed by means of a computer system

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of insulting a person for the reason that he or she belongs to a group distinguished by race, colour, descent, national or ethnic origin or religion, if used as a pretext for any of these factors, or a group of persons distinguished by any of these characteristics.

Section 10
Offences related to terrorism, weapons manufacture or trafficking in persons or drugs, committed with the help of a computer or a computer system

§1. Creation or publication of a site for terrorist groups

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of:

1. Establishing, publishing or using the website of a terrorist group with the aid of the Internet, a computer or a computer system in order to facilitate communication by its leadership or members;

2. Raising funds or disseminating its ideas or knowledge about how it conducts its terrorist operations.

§2. Dissemination of methods or means of destruction

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of disseminating or making available to others through a computer system, except to authorized persons, instructions for use or methods for the manufacture of firearms, their parts and components and ammunition of such nature as to cause harm to human life, property or the environment.

§3. Creation or publication of a site for the purpose of trafficking in human beings

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of establishing or publishing a site on an information network, computer equipment or a computer system for the purpose of trafficking in persons or facilitating such a transaction.

§4. Creation or publication of a site for the purpose of trafficking in or distributing drugs or narcotics

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of creating or publishing a site on an information network, computer equipment or a computer system for the purpose of trafficking in or distributing drugs or narcotics or facilitating such a transaction.

Section 11
Computer-related criminal association

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the act of intentionally participating in an association formed or a conspiracy established for the purpose of preparing or committing one or more offences.

Section 12
Offences related to infringements of intellectual property and related rights

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, any infringement of intellectual property rights.

Chapter III. Liability of legal persons

The States Parties to this Convention shall undertake such arrangements as may be necessary to ensure that legal persons can be held liable for the offences established by this Convention.

Take the measures necessary to ensure that a legal person can be held liable for lack of supervision or control by a natural person working within that legal person. The liability of a legal person may be criminal, civil or administrative.

Canada

[Original: English]
[9 April 2022]

Offences

Illegal access to a computer system

Establish as a criminal offence to, fraudulently and without right, access the whole or any part of a computer system.

Illegal interception of non-public computer system transmission

Establish as a criminal offence to, fraudulently and without right, intercept, by any technical means, non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such data.

Computer data interference

Establish as a criminal offence to, intentionally and without right, damage, delete, deteriorate, alter or suppress computer data.

Computer system interference

Establish as a criminal offence to, intentionally and without right, seriously hinder the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Misuse of devices

1. Establish as criminal offences, 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 cybercrime offences included in this Convention;

(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 cybercrime offences included in the convention; and

(b) The possession of an item referred to in paragraph 1 (a)(i) or (ii), with intent that it be used for the purpose of committing any of the cybercrime offences included in this Convention.

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 is not for the purpose of committing a cybercrime offence included in this Convention, such as for the authorized testing or protection of a computer system.

Child sexual exploitation-related offences

1. Establish as criminal offences, when committed intentionally and without right, the following conduct:

(a) Producing child sexual exploitation material for the purpose of its distribution through a computer system;

(b) Offering, advertising or making available child sexual exploitation material through a computer system;

(c) Distributing or transmitting child sexual exploitation material through a computer system;

(d) Procuring child sexual exploitation material through a computer system for oneself or for another person;

(e) Accessing or possessing child sexual exploitation material in a computer system or on a computer data storage medium.

2. For the purpose of paragraph 1, the term “child sexual exploitation material” includes child pornography as defined in the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and any:

(a) Visual material, including photographic, video and live-streaming media, that depicts:

(i) A child engaged in or in the presence of sexual activity;

(ii) A person appearing to be a child engaged in or in the presence of sexual activity;

(iii) Realistic images representing a child engaged in or in the presence of sexual activity;

(b) Written material that:

(i) Advocates sexual activity with a child;

(ii) Is written for a sexual purpose and has as a dominant characteristic the description of sexual activity with a child; and

(c) Audio recordings that:

(i) Advocates sexual activity with a child;

(ii) Is recorded for a sexual purpose and has as a dominant characteristic the description of sexual activity with a child.

Grooming and luring of a child

1. Establish as criminal offences, when committed intentionally and without right, the following conduct:

(a) Transmitting, distributing, selling or making available through a computer system sexually explicit material to a child or a person believed to be a child;

(b) Communicating with a child, or a person believed to be a child, through a computer system; or

(c) Agreeing or making arrangements with a child, or a person believed to be a child, through a computer system;

for the purpose of facilitating the commission of any child sexual exploitation offences established under this Convention, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography or the domestic law of the State Party.

2. No criminal liability is established if a person has taken reasonable steps to ascertain the person is not a child.

Non-consensual dissemination of intimate images ("revenge porn")

1. Establish as criminal offences, when committed intentionally and without right, publishing, distributing, transmitting, selling, making available or advertising an intimate image of a person by any means of a computer system, 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 depicted retains a reasonable expectation of privacy at the time the offence is committed.

3. No criminal liability is established if the non-consensual sharing is for the public good or has a legitimate purpose.

Colombia

[Original: Spanish]
[8 April 2022]

3. Criminalization

With regard to cyber-dependent crimes, each Member State should adopt such legislative and other measures as may be necessary to establish as criminal offences, in its domestic legal system, the following acts:

(a) Illegal access: Accessing without right the whole or any part of a computer system.[22]

[22] Article 2 of the Budapest Convention on Cybercrime. Consistent with article 269A of Act No. 1273 of 2009.

(b) Illegal interception: The interception without right of computer data, whether at its origin or destination or within a computer system, or in the electromagnetic emissions from a computer system carrying such data.[23]

(c) Data interference: The damaging, destruction, deletion, deterioration, alteration or suppression of computer data or of an information processing system or the logical components or parts thereof.[24]

(d) System interference: The hindering without right of the functioning of or normal access to a computer system, the data contained therein or a telecommunications network.[25]

(e) Misuse of devices: The production, procurement, possession or distribution of, or trading in, a device, including a computer program, as well as a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, for the purpose of committing any of the offences referred to in paragraphs (a), (b), (c) and (d) of this section.[26]

(f) Computer-related forgery: The intentional inputting, alteration, deletion or suppression without right 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.[27]

With respect to cyber-enabled crimes, each Member State should adopt such legislative and other measures as may be necessary to establish as criminal offences, in its domestic legal system, the following acts:

(a) Offences related to child sexual abuse material: The production, offering, distribution, transmission or procurement of child sexual abuse material through, or the possession of such material in, a computer system.[28]

(b) Computer-related fraud: The inputting, alteration, deletion or suppression of computer data, or interference with the functioning of a computer system, with the fraudulent or criminal intent of procuring, without right, an economic benefit for oneself or for another person, to the detriment of another person's property.[29]

(c) Violation of personal data: The unauthorized obtaining, compilation, removal, offering, sale, exchange, sending, purchase, interception, disclosure, modification or use, for personal gain or for the gain of a third party, of personal data contained in files, archives, databases or similar media.[30]

natural persons and monetary sanctions in the case of legal persons.[31]

[23] Article 3 of the Budapest Convention on Cybercrime. Consistent with article 269C of Act No. 1273 of 2009.

[24] Article 4 of the Budapest Convention on Cybercrime. Consistent with article 269D of Act No. 1273 of 2009.

[25] Article 5 of the Budapest Convention on Cybercrime. Consistent with article 269B of Act No. 1273 of 2009.

[26] Article 6 of the Budapest Convention on Cybercrime.

[27] Article 7 of the Budapest Convention on Cybercrime.

[28] Article 9 of the Budapest Convention on Cybercrime.

[29] Article 8 of the Budapest Convention on Cybercrime.

[30] Article 269F of Act No. 1773 of 2009.

[31] Article 13 of the Budapest Convention on Cybercrime. Consistent with article 30 of the United Nations Convention against Corruption and article 11 of the United Nations Convention against Transnational Organized Crime.

Egypt

[Original: Arabic]
[8 April 2022]

Chapter II
Criminalization, criminal proceedings and law enforcement

Article 5
Criminalization

1. Each State party shall adopt such legislative and other measures as are necessary to prevent and detect the commission of the offences set forth in this Convention or any other offences committed through information and communications technologies, including blocking and removing content related to such offences, prosecuting the perpetrators thereof, extraditing offenders, facilitating international cooperation procedures and gathering evidence in respect of such offences, while affirming the importance of the principle of technological neutrality.

2. Each State party shall also adopt such legislative and other measures as are necessary to criminalize the following acts:

Article 6
Unlawful use or facilitation of the unlawful use of communication and information services and technologies

The illegal use or facilitation for others of the use of communication services or audio or video broadcasting channels through an information network or information and communications technologies.

Article 7
Unlawful access and/or exceeding of the limits of the right of access

1. A person's exceeding of the time limits or access-level limits of a right granted to that person to access a website, private account or information system.

2. Unlawful access of, presence in or contact with all or part of an information technology or the perpetuation thereof.

3. The penalty shall be increased if such access, presence, contact or perpetuation results in:

(a) The erasure, modification, distortion, copying, transfer or destruction of saved data, electronic devices or systems or communication networks, or the causing of harm to users and beneficiaries;

(b) The obtainment of confidential government information.

Article 8
Attack on a site design

The unlawful damaging, disruption, slowing, distortion, concealment or modification of the site design of a company, institution, establishment or natural person.

Article 9
Unlawful interception

The intentional, unlawful interception of a data flow by any technical means, or the disruption of the transmission or reception of information technology data.

Article 10
Attack on data integrity

The intentional, unlawful destruction, erasure, obstruction, modification or blocking of information technology data.

Article 11
Misuse of information technology

The production, sale, purchase, importation, distribution, provision or possession of any designed or adapted tools or software, password or similar information by which an information system may be accessed with the intent of using it to commit an offence under this Convention, or the creation of malicious software intended to destroy, block, modify, copy or disseminate digital information or to neutralize the security features of digital information, except for legitimate research.

Article 12
Falsification

The use of information technology to change the substance of data with the intent of using the data as valid data in a way that would cause harm.

Article 13
Fraud

The intentional, unlawful causing of harm to beneficiaries and users with the intent of fraud to realize interests and benefits in an illegal way for the perpetrator or others, including through fraudulent electronic crimes related to virtual currencies (digital or encrypted).

Article 14
Threat and blackmail

The use of information and communications technologies or any other technical means to threaten or blackmail a person into committing an act or refraining from performing an act.

Article 15
Pornography

1. The production, display, distribution, provision, publication, purchase, sale or importation of pornographic material for the purpose of prostitution or exploitation of women or minors through information and communications technologies, according to the domestic law of each State.

2. The production, display, distribution, provision, publication, purchase, sale or importation of pornographic material depicting children or minors, including the possession of material depicting children or minors that is deemed obscene, on information and communications technologies or a medium for the storage of information and communications technologies.

Article 16
Other offences related to pornography

Sexual exploitation or harassment, especially of women, children or minors.

Article 17
Encouragement or coercion to commit suicide

The encouragement or coercion, including of minors, to commit suicide, through psychological or other pressure over information and communication networks,

including the Internet, whether through direct interaction or through modern technologies and electronic games.

Article 18
Involvement of minors in the commission of illegal acts

The involvement of minors, through information and communications technologies, in the commission of illegal acts that endanger their lives or their physical or mental health.

Article 19
Violation of privacy

Violation of privacy using information and communications technologies, including the creation of an email, website or private account and falsely attributing it to a natural or legal person.

Article 20
Terrorism-related offences committed using information technology

1. Dissemination, advocacy or justification of the ideas and principles of terrorist groups.

2. Financing of or training for terrorist acts, facilitation of communication between terrorist organizations or the provision of logistical support for perpetrators of terrorist acts.

3. Dissemination of methods for making explosives employed in particular in terrorist acts.

4. Spreading of strife, sedition, hatred or racism.

5. States shall take the necessary measures to prevent the dissemination of such content via information and communications technologies, including blocking or removing content related to these offences.

Article 21
Financial offences, including money-laundering

1. Use of information and communications technologies to commit financial offences, or the misuse of virtual currencies (digital and encrypted).

2. Conduct of money-laundering operations, requesting of assistance to conduct money-laundering operations, or the publication of money-laundering methods.

Article 22
Illicit use of electronic payment instruments

1. The forging, fabrication or installation of any device or materials that facilitate the forgery or imitation of any electronic payment instrument by any means.

2. Appropriation, use or provision to others of the data of any payment instrument, or the facilitation of the obtainment of such data by others.

3. The use of an information network or information technology to gain unauthorized access to the numbers or data of any payment instrument.

4. The knowing acceptance of a forged payment instrument.

Article 23
Offences related to organized or transnational crime committed using information technology

1. Promotion of or trafficking in narcotic drugs or psychotropic substances.

2. Illicit distribution of counterfeit medicines or medical products.

3. Smuggling of migrants.

4. Illicit trafficking of persons or human organs.

5. Illicit arms trade.

6. Illicit trafficking in cultural property.

Article 24
Offences related to infringement of copyright or related rights

Violation of copyright or related rights as defined in the law of the State party, if the violation is committed intentionally.

Article 25
Unauthorized access to critical information infrastructure

1. The creation, distribution or use of software or other digital information designed to provide unauthorized access to a critical information infrastructure, including the destruction, blocking, modification or copying of the information contained therein or the neutralization of security features.

2. Violation of the rules of use for media that have been designed for the storage, processing or transfer of protected digital information that is present in critical information infrastructure or information systems according to the domestic law of the State party, information and communication networks that belong to critical information infrastructure or the means of access thereto, if such violation harms the critical information infrastructure.

Article 26
Incitement to subversive or armed activities or other criminal offences

Calls issued through information and communications technologies advocating sabotage or armed activities directed against the regime of another State that would destabilize public security and stability; or the commission of criminal offences punishable by imprisonment of at least one year.

Article 27
Offences related to extremism

The distribution of materials that call for illegal acts with political, ideological, social or ethnic motives or any other illegal act advocating ethnic or religious hatred or hostility in general, by means of information and communications technologies, or the advocacy, justification or provision of access to it.

Article 28
Attempted commission or participation in the commission of an offence

The attempted commission or commission of a criminal offence set forth in the Convention, and/or participation as an accomplice in a criminal offence set forth in the Convention, and/or the organization or directing of other persons to commit a criminal offence set forth in the Convention.

Article 29
Other illegal acts

This Convention shall not prevent a State party from criminalizing any other illegal act committed intentionally through information and communications technologies.

Article 30
Liability of legal entities

1. Each State party shall undertake, subject to its domestic law, to regulate the criminal liability of legal persons for offences committed by their representatives in their name or for their benefit, without prejudice to the punishment of natural persons, including site administrators, who commit offences.

2. Without prejudice to the provisions of this Convention, service providers/site administrators and their affiliates shall abide by the following obligations, the breach of which shall be considered an offence:

(a) The saving and storage of the following data in an information system log or information technology log for a period of (to be determined):

- Data that enable the identification of service users
- Data related to the content that is processed on information systems when such data are under the control of the service provider
- Data related to communication traffic
- Data related to communication peripherals
- Any other data specified by the State for the purposes of implementing this Convention

(b) Maintenance of the confidentiality of saved and stored data, and refraining from disclosing the data without a reasoned order from the competent authorities, including the personal data of any of its service users, any data or information related to the sites and private accounts accessed by its users, and the persons or entities with whom its users communicate;

(c) Securement of the data and information in a manner that maintains the confidentiality thereof and protects the data and information from being penetrated or damaged;

(d) Provision of easy, direct and continuous access to the following data and information for users of its services and any competent authority:

- The name and address of the service provider
- The contact information of the service provider, including its email address
- Licensing data that identifies the service provider and the competent authority that supervises it

(e) The provision, upon the request of the competent authorities specified by the State, of all technical capabilities needed to enable such authorities to exercise their powers.

El Salvador

[Original: Spanish]
[12 April 2022]

Provisions on criminalization

States should adopt appropriate legislative and other measures to establish as criminal offences under their national law – imposing criminal and other sanctions, including imprisonment, that take into account the number of victims and the extent of the damage caused – the following acts:

Illegal access

When committed intentionally, access to the whole or any part of a computer system without due authorization. This does not apply to authorized tests or investigative activities that are legitimate and verifiable, provided that they do not cause serious indirect damage.

Unlawful interception

When committed intentionally and without right, the interception without due authorization, carried out 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.

Data interference

When committed intentionally and without right, the damaging, deletion, deterioration, alteration or suppression of computer data without due authorization.

Interference with computer systems

When committed intentionally and without right, the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Misuse of devices

When committed intentionally and without right, the production, sale, acquisition for use, import, distribution or making available of any device, including computer programs, designed or adapted primarily for the purpose of committing any of the offences set forth in this Convention; or passwords, access codes or similar data by which the whole or part of a computer system is capable of being accessed for the purpose of committing any of the offences established in this Convention. This does not apply to authorized tests or investigative activities that are legitimate and verifiable, provided that they do not cause serious indirect damage.

Computer-related forgery

When committed wilfully and without right, the inputting, alteration, deletion or suppression of computer data, resulting in inauthentic data, regardless of whether the data are directly readable and intelligible. Intent to defraud, or similar dishonest intent, may be required before criminal liability attaches.

Fraud committed by means of information and communications technologies

When committed wilfully and without right, acts that cause damage to another person’s property through any entry, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring an economic benefit for oneself or for another person.

Offences related to material with child abuse content

When committed wilfully and without right, the following conduct: producing, reproducing, distributing, publishing, importing, exporting, offering, financing, selling, marketing, disseminating or possessing such content on any type of technological device or medium.

Infringement of intellectual property and related rights

The infringement of intellectual property and related rights as defined in the legislation of the State Party when such acts are premeditated and committed through the use of information and communications technologies, including the unlawful use

of computer programs and databases, which are protected by copyright, and plagiarism.

Aiding or abetting and attempt

Participation as an accomplice, aider or instigator, or in any other role, in an offence; any attempt to commit an offence or the preparation for an offence established in accordance with this Convention.

Liability

Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in this Convention where such offences are committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a power of representation of the legal person; an authority to take decisions on behalf of the legal person; an authority to exercise control within the legal person.

In addition to the cases provided for in the preceding paragraph, 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 the preceding paragraph has made possible the commission of an offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

Subject to the legal principles of the State Party, such liability may be criminal, civil or administrative. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

Each State Party shall, in particular, ensure that legal persons held liable in accordance with this Convention are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Prosecution, adjudication and sanctions

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

Each State Party shall endeavour to ensure that any discretionary legal power under its domestic law relating to the prosecution of persons for offences covered by this Convention is 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.

In the case of offences established in accordance with the articles of this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the 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.

Each State Party shall ensure that its courts or other competent authorities bear in mind the gravity of the offences covered by this Convention when considering the eventuality of early release or parole of persons convicted of such offences.

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

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 exceptions or other legal principles governing 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.

Laundering of proceeds of offences committed through the use of information and communications technologies

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, the following:

(a) The conversion or transfer of property, 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 action;

(b) 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;

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

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

For the purposes of implementing or applying the provisions of this paragraph, each State Party shall endeavour to:

(a) Apply the provisions of this paragraph to the widest range of predicate offences;

(b) Include as predicate offences the offences established in accordance with the articles of 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 organized criminal groups;

(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 when 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.

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, the following:

(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 right of States Parties to have legislation that protects other categories of public officials.

Jurisdiction

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:

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

(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.

A State Party may also establish its jurisdiction over any such offence when:

(a) The offence is committed against a national of that State Party;

(b) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory;

(c) The offence is committed against a State Party.

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.

If a State Party exercising its jurisdiction in accordance with the preceding paragraphs has been notified, or has otherwise learned, that another State Party is 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.

Without prejudice to norms of general international law, this Convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

European Union and its member States

[Original: English]
[6 April 2022]

Chapter II
Criminalization and law enforcement

Article 5
Illegal access

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the access to the whole or any part of a computer system without right where committed by infringing a security measure.

2. A State Party may require that the offence be committed 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 6
Illegal interception

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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.

2. A State 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 7
Illegal data interference

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

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

Article 8
Illegal system interference

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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 9
Misuse of devices

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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 article 5 through 8 of this Convention;

(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 article 5 through 8 of this Convention; and

(b) The possession of an item referred to in paragraph 1 (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in article 5 through 8 of this Convention. A State Party may require 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 5 through 8 of this Convention, such as for the authorized testing or protection of a computer system.

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

Article 10
Attempt and aiding and abetting

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 5 to 9 of this Convention.

2. Each State Party may adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 5 to 9 of this Convention.

Article 11
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 ensure that legal persons can be held liable for a criminal offence established in accordance with Articles 5 to 10 of this Convention.

2. Subject to the legal principles of the Party, the liability of a legal person 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.

Article 12
Prosecution, adjudication and sanctions

1. Each State Party shall make the commission of an offence established in accordance with articles 5 to 10 of this Convention liable to effective, proportionate and dissuasive sanctions for both natural and legal persons.

2. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by 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.

3. Each State Party shall develop and maintain an effective and rule of law-based national criminal justice system that can ensure that any person prosecuted for offences covered by this Convention is brought to justice whilst ensuring full protection of human rights and fundamental freedoms, including the right to a fair trial and the rights of the defence.

Ghana

[Original: English]
[12 April 2022]

Chapter II. Provisions on criminalization[32]

Cyber-dependent crimes: offences against the confidentiality, integrity and availability of computer systems and data

Article 5
Unauthorized access to a computer system

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally: the access to the whole or any part of a computer system, without authorization or exceeding authorized access. 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 6
Unauthorized access to a critical information infrastructure

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally: the access to the whole or any part of a critical information infrastructure without authorization.

Article 7
Unauthorized 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 authorization, 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, copying or suppression of computer data without authorization.

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

[32] The text for this section is adopted from primarily the Council of Europe Convention on Cybercrime, the African Union Convention on Cyber Security and Personal Data Protection, the Electronic Transactions Act, 2008 (Act 772) and the Cybersecurity Act, 2020 (Act 1038). These instruments form the cybercrime legislative framework of Ghana.

intentionally, the serious hindering without authorization 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 5 through 9;

(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 5 through 9; and

(b) The possession of an item referred to in paragraph 1 (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in articles 5 through 9. 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 5 through 9 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.

Cyber-enabled crimes: offences whose scope, speed and impact have increased as a result of the advent of computer systems[33]

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 are 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:

[33] Computer related fraud, forgery and crimes targeting children are consistent with Council of Europe Convention on Cybercrime, the African Union Convention on Cyber Security and Personal Data Protection and the Cybersecurity Act, 2020 (Act 1038).

(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.

Crimes against children

Article 13
Offences related to child sexual exploitation and abuse online

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 sexual exploitation and abuse material for the purpose of publication and distribution through a computer system;

(b) Procuring child sexual exploitation and abuse material for oneself or for another person;

(c) Offering or making available child sexual exploitation and abuse material through a computer system or an electronic device;

(d) Publishing, distribution, streaming (including live streaming), transmitting child sexual exploitation and abuse material through a computer or an electronic device or;

(e) Possessing child sexual exploitation and abuse material in a computer system or on a computer or electronic record storage medium.

2. For purpose of paragraph (c) of subsection (1), a person publishes child sexual exploitation and abuse material if that person:

(a) Parts with possession of the child sexual exploitation and abuse material to another person; or

(b) Exposes or offers the child sexual exploitation and abuse material for acquisition by another person.

3. For the purpose of this section, child sexual exploitation and abuse material includes a material image, visual recording, video, audio, live streaming material, drawing or text, that depicts or describes:

(a) A child engaged in sexually explicit or suggestive conduct;

(b) A person who appears to be a child engaged in sexually explicit or suggestive conduct;

(c) Images representing a child engaged in sexually explicit or suggestive conduct;

(d) Sexually explicit images of children;

(e) Process or material for viewing of child sexual exploitation and abuse in real-time often involving the offender directing the abuse;

(f) Any written material, visual representation or audio recording that advocates or counsels unlawful sexual activity with children;

(g) Any written material that has, as its dominant characteristics, the description, for a sexual purpose of unlawful sexual activity with a child;

(h) Any audio recording that has as its dominant characteristic, the description, for a sexual purpose, of unlawful sexual activity with a child.

Article 14
Dealing with a child for purposes of sexual abuse

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 use of:

(a) A computer online service;

(b) An Internet service;

(c) A local bulletin board service; or

(d) Any other device capable of electronic data storage or transmission;

to seduce, solicit, lure, groom or entice or attempt to seduce, solicit, lure, groom or entice a child or another person believed by the person to be a child, for the purpose of facilitating, encouraging, offering or soliciting unlawful sexual conduct of or with any child, or the visual depiction of such conduct.

Article 15
Cyberstalking of a child

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 use of a computer online service, an Internet service or a local Internet bulletin board service or any other electronic device 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.

Other online sexual offences[34]

Article 16
Sexual extortion

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 threatening to distribute by post, email, text or transmit, by electronic means or otherwise, a private image or moving images of another person engaged in sexually explicit conduct, with the specific intent to:

(a) Harass, threaten, coerce, intimidate or exert any undue influence on the person especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or

(b) Actually extort money or other consideration or compel the victim to engage in unwanted sexual activity.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the threatening to distribute by post, email, text or transmit, by electronic means or otherwise, a private image or moving images of a child engaged in sexually explicit conduct, with the specific intent to:

(a) Harass, threaten, coerce, intimidate or exert any undue influence on the child especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or

[34] Consistent with provisions of the Cybersecurity Act.

(b) Actually extort money or other consideration or compel the victim to engage in unwanted sexual activity.

3. For the purpose of paragraphs 1 and 2, an intimate image may include a depiction in a way that the genital or anal region of another person is bare or covered only by underwear; or the breasts are shown below the top of the areola, which is either uncovered or clearly visible through clothing.

Article 17
Non-consensual sharing of intimate image

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the intentional distribution of, or intentionally causing another person to distribute, the intimate image or prohibited visual recording of another identifiable person, without the consent of the person depicted in the intimate image, with the intent to cause serious emotional distress and in respect of which there was a reasonable expectation of privacy either at the time of the creation of the image or visual recording and/or at the time the offence was committed.

2. For the purpose of this section, "serious emotional distress" includes any intentional conduct that results in mental reactions such as fright, nervousness, grief, anxiety, worry, mortification, shock, humiliation and indignity, as well as physical pain.

Article 18
Threat to distribute prohibited intimate image or visual recording

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, threatening to distribute a prohibited intimate image or visual recording of another person in a way that would cause that other person distress reasonably arising in all circumstances, and the threat is made in a way that would cause that other person fear, reasonably arising in all circumstances, of the threat being carried out.

Article 19
Offences related to infringements of copyright and related rights[35]

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 relating to the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the World Intellectual Property Organization (WIPO) Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (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

[35] Consistent with the Council of Europe Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection.

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 20
Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with articles 5 through 19 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with articles 7 through 9; 11; 12; 13, paragraph 1 (a), (b) and (e); 14; 15; 16; and 17.

Article 21
Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

(a) A power of representation of the legal person;

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

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

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

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

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

Article 22
Sanctions and Measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with articles 5 through 20 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with article 21 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Iran (Islamic Republic of)

[Original: English]
[8 April 2022]

2. Criminalization

It is increasingly the case that offenders organize and carry out unlawful activities not only against but through information and communications technology devices. Though criminal acts may be established as offences notwithstanding misuse of ICT or vice versa, in certain cases the gravity and other factors surrounding the offence requires criminalizing the unlawful act when conducted via the use of information and communications technology. This is especially the case when use of information and communications technology intensifies the commission of crimes in terms of, inter alia, the extent of harm it inflicts upon victims. Therefore, in addition to crimes dependent on information and communications technology, crimes enabled by these technologies should be criminalized within the convention. Nonetheless, from a legal standpoint this may require a case-by-case approach since various forms of crime may reflect differentiated elements, as well as actus reus and mens rea. In adopting measures for establishing offences due regard should be had as to the fundamental principles of domestic legal systems.

Liability of legal persons should also be established to ensure a comprehensive response to criminal activities and to deny offenders of freedom of operation under the veil of legal entities. Such measure should hold legal persons liable for deliberate or otherwise knowing involvement in the commission of offences to be established in accordance with the convention.

Japan

[Original: English]
[8 April 2022]

1. Criminalization

1.1. Cyber-dependent crimes

1.1.1. Japan recognizes that there is general consensus in the Ad Hoc Committee on the criminalization of cyber-dependent crimes, which consist mainly of offences that violate the confidentiality, integrity and availability of computer data and systems. Based on this recognition, Japan supports the criminalization of cyber-dependent crimes.

1.1.2. We believe that many of the acts that need to be criminalized to address today's challenges to which each Member State attaches importance, such as ransomware attacks and attacks on computer systems of critical infrastructure, are in the range of cyber-dependent crimes. Such cyber-dependent crimes could include illegal access, illegal interception, interference with computer data or computer systems and misuse of devices, among others.

1.1.3. Japan recognizes the importance of countermeasures against attacks on the computer systems of information infrastructures and facilities. However, since these attacks, such as theft or alteration of data through hacking, can be considered within the scope of cyber-dependent crimes, there is no need to deal with these offences as issues specific to information infrastructures or facilities. Also, as it is important to make the forthcoming convention applicable for the long-term future, it should be noted that provisions on criminalization will lose their versatility if they are too focused on individual modi operandi. Furthermore, it is important that this new convention stipulate basic and essential provisions that could be complied with and implemented by as many Member States as possible. In light of this, the discussion

should start with common cybercrimes such as illegal access. It should be carefully considered whether or not it is necessary to establish a specific provision for attacks on computer systems of information infrastructures and facilities in addition to provisions on common cybercrimes in order to avoid duplication among provisions on criminalization.

1.1.4. In addition, it is necessary to avoid the risk of a chilling effect on legitimate operations and activities, such as technology development, or abuse of power by law enforcement authorities caused by an overly broad scope of criminalization. For example, when criminalizing illegal access, it may be required that there be no legitimate reason for the access and awareness of that, in order to avoid imposing absolute liability.

1.1.5. Furthermore, mandating uniform punishment for attempted crimes or aiding and abetting crimes, or mandating punishment at the stage of preparation or conspiracy that is not sufficient to constitute an attempt, would be an excessive interference with the domestic criminal legislation of individual States. The criminalization of these offences should be left to the national legislation of each Member State. Regarding countermeasures against cybercrimes that have a transnational nature, it is very important not to create a safe haven for cybercrime. Therefore, it is necessary to avoid stipulating such provisions that limit the number of Member States that can conclude the new convention due to differences in the basic legal concepts that inevitably exist among Member States.

1.2. Freedom of expression

1.2.1. In considering the criminalization of activities in cyberspace, reference should be made to international human rights treaties. In determining what acts can be criminalized as cyber-enabled crimes under the new convention, particularly with regard to the criminalization of acts related to harmful content on the Internet, Member States must not forget the importance of protecting freedom of expression.

1.2.2. For example, article 19, paragraph 2, of the International Covenant on Civil and Political Rights stipulates that freedom of expression “shall include 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 his choice.” While keeping in mind that article 19, paragraph 3, provides for certain restrictions to the right, we must ensure that there is room for the development of domestic laws considering the actual situation in each Member State so that the rights and freedoms relating to academic research, cultural and artistic activity, and press are not unjustly infringed upon.

1.2.3. In order to protect freedom of expression, it is necessary to avoid causing a chilling effect on expressive activities. Therefore, criminalization of acts related to harmful content on the Internet should be undertaken only to the extent that all Member States can agree on the definition of such acts, and that there are demonstrable grounds for the need for punishment.

1.2.4. In order to make this Convention a treaty that as many Member States as possible can conclude, and to await for the discussions to ripen internationally as well as nationally, we believe that one of the most promising options would be to leave the criminalization of acts pertaining to harmful content to a future additional protocol.

1.3. Conventional crimes exploiting cyberspace

1.3.1. Regarding crimes related to terrorism, firearm-related offences and drug-related offences, they may constitute convention crimes even when they are committed via the use of the Internet, and existing treaties such as the United Nations Convention against Transnational Organized Crime may also apply.

1.3.2. Criminalization of these acts should be carefully considered so as not to duplicate above-mentioned existing efforts. Reference should also be made to the

discussions during the process of formulation of existing treaties so that provisions that were intentionally not included in them will not simply be incorporated in this Convention in a different form.

1.4. Possible cyber-enabled crimes to be considered

With regard to cyber-enabled crimes other than those regarding harmful content (see 1.2 above), some cyber-enabled crimes that are recognized as significant to be criminalized as cybercrimes under this Convention could be subject to discussion on criminalization, under the premise that all Member States can agree on a definition of such acts and that there are demonstrable grounds for the need for punishment. Such cyber-enabled crimes include those whose scope and speed and scale of damages are increased by the use of computers. These crimes may include offences as follows.

1.4.1. Computer-related forgery

It is difficult to detect computer data forgery with the human senses. Moreover, in today's world where many business processes are carried out by computer, the social impact of undermining trust in computer data is significant. Therefore, Japan could support the criminalization of the input, alteration, deletion or suppression of computer data, resulting in inauthentic data, when committed intentionally and without right.

1.4.2 Computer-related fraud

Computer data fraud, when perpetrated through the forgery of computer data or through interference with the functioning of computer systems, is easy to perpetrate against a wide range of targets and can cause serious property damage in many Member States. Therefore, we could support the criminalization of the causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring.

1.4.3 Infringements of copyright

On the Internet, data can be copied and content can be reproduced easily, and such content spreads fast, which can increase the degree of copyright infringement. We believe that it would be beneficial to criminalize the infringement of copyright and related rights where such acts are committed wilfully, on a commercial scale and by means of a computer system, with reference to existing international agreements related to copyright.

1.4.4 Child sexual abuse and exploitation

The production and distribution of child sexual abuse materials are extremely malicious acts that have a harmful effect on the mental and physical health of depicted children and seriously infringe upon their human rights. It is difficult to delete child sexual abuse materials once they have been disseminated through the Internet, and they will continue to have a serious impact on the sound upbringing of the children. From the perspective of protecting human rights of children, we support the criminalization of the production and distribution of materials that visually depict a child engaged in sexually explicit conduct.

Nevertheless, we believe that careful consideration should be given to treating realistic images representing a person appearing to be a minor or a non-existing child engaged in sexually explicit conduct as child sexual abuse materials and criminalizing offences related to these images, taking into account that an existing minor is not subject to direct abuse as well as the importance of freedom of expression.

1.5. Liability of legal persons

We support stipulating the liability of legal persons to a certain extent in cases where such legal persons organizations widely committed cybercrimes with regard to their business under the condition that the liability may be criminal, civil or administrative subject to the legal principles of each Member State. The division of roles among criminal, civil, and administrative matters and the necessity of sanctions are issues that should be left to the domestic legislation of each Member State, as they need to be considered in light of each Member State's national structure and the parity with governance outside the cyber sector in each Member State.

Jordan

[Original: Arabic]
[7 April 2022]

The Hashemite Kingdom of Jordan proposes that the following acts should be criminalized under the draft convention:

- Unlawful access to an information network, information system or any part thereof by any means, without authorization or in violation of authorization. The penalty for this offence should be increased in cases of unlawful access to an information network, information system or any part thereof that belongs to an official, public, security, financial or banking institution and unlawful access to critical infrastructure and data or information not available to the public that affects national security, the foreign relations of the State, public safety or the national economy.
- Illegal interception of data traffic.
- The violation of data or information related to electronic payment methods, the execution of electronic financial or banking transactions or the transfer of funds through an information network or information system.
- Electronic fraud.
- IP address fraud.
- Sexual exploitation through information systems, networks or websites.
- Dissemination of rumours or false news through information systems, networks or websites.
- Hate speech or actions related to the insulting of religions or States using information networks or websites.
- Unlawful interference with information systems or information networks by implanting or introducing malicious software.
- The creation of a website similar to a real website to mislead or deceive users for the purpose of stealing login data or personal information or collecting unlawful donations.
- The sending of emails or text messages with the aim of phishing for the purposes of data theft, spreading malicious software or attempting to access networks or information systems to which access is not permitted.
- The creation of fake pages, groups or accounts on social media sites to mislead or deceive users, collect unlawful donations or engage in electronic begging.
- The targeting of users' devices to create an information network without the users' knowledge to use it for denial-of-trust attacks or unlawful purposes.

- The exploitation or attempted exploitation of security vulnerabilities in information networks or systems with the intent of penetrating them or stealing, destroying or modifying data.
- The scanning or attempted scanning of Internet protocols or network access ports without permission with the intent to collect information or identify security vulnerabilities.
- The unauthorized use of hardware or software for guessing passwords or usernames.
- The use of artificial intelligence technology to commit unlawful acts.
- Acts related to impersonation.
- Acts relating to breach of privacy.
- Acts related to intellectual property and software piracy.
- Acts that constitute an attack on supply chains.
- Acts related to the unauthorized use of data by service providers.
- Acts related to the dissemination, support or promotion of a terrorist ideology.
- Acts related to the use of information and communication technologies for terrorist purposes.
- Acts related to electronic fraud.
- Acts related to the marketing or trafficking of drugs by electronic means.
- Acts related to money-laundering by electronic means.

Mexico

[Original: English]
[13 April 2022]

Criminalization

National jurisdiction will be a fundamental element to define criminalization obligations. In this regard, Mexico considers that the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption offer examples of provisions applicable by extension to countering crimes related to the use of information and communications technologies, except for those cases linked to information in the cloud, which will require further analysis and discussion from recent experiences of concrete investigations.

A departing point for criminalization should be to consider in the Convention those behaviours recognized by international law as crimes, particularly in the terms provided by other treaties adopted within the framework of the United Nations, which are carried out by information and communications technologies and electronic and digital means. Thus, it is recommended to include the following article:

> "*States Parties recognize as crimes for the purposes of this Convention, all criminal acts recognized by the existing international law that are perpetrated by information technologies and electronic means.*"

Among other criminal offences, for the Government of Mexico it will be crucial to include those crimes related to child sexual exploitation as well as those related to gender violence by the means of information and communications technologies.

It is recommended to include operative elements to strengthen investigation and prosecution; then it will be relevant to consider including annexes with those templates specifying needed data to proceed with information-sharing requests.

As it is not expected to list all kinds of criminal offences but primarily cyber-dependent crimes, and in order to prevent incompatibility or duplications of national laws, it is recommended to include a general commitment by States Parties to harmonize their legislations, if needed.

> "*Nothing in this Convention shall affect the rights, obligations and responsibilities of States and individuals under existing international law aimed to prevent and counter the use of information and communications technologies for criminal purposes.*"

> "*In all actions aimed at the implementation of the present Convention, the best interests of the victims – individuals and institutions and organizations – of the crimes recognized in the present Convention shall be a primary consideration.*"

New Zealand

[Original: English]
[8 April 2022]

Criminalization provisions

1. During the first session, we heard widespread support for, and no opposition to, the inclusion of provisions targeting cybercrime within this Convention, particularly cyber-dependent crimes and a limited range of cyber-enabled crimes.

2. In annex 1 of this document, we propose a list of criminalization provisions that New Zealand believes have the greatest likelihood of achieving consensus and should therefore be the focus of the Ad Hoc Committee's attention, given the limited resources and limited time. We also provide some text suggestions to assist with drafting, primarily drawn from other relevant international instruments such as the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and the Council of Europe Convention on Cybercrime (Budapest Convention).

3. New Zealand supports including a provision on jurisdiction that mirrors, where applicable, existing instruments, such as article 42 of the United Nations Convention against Corruption, with additional elements requiring States to exercise jurisdiction where the offence or any part of the offence is committed in the territory of the State party, to reflect the reality that cybercrimes may be committed in cyberspace, with the possibility that the perpetrator, victim, data and computer system used are in different jurisdictions.

Annex 1 – Criminalization provisions

Illegal access to computer systems

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.

Illegal interception of computer data

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.

Interference with computer data

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.

Interference with the functioning of computer

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.

Misuse of devices or computer programs

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 [relevant articles];

(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 the intent that it be used for the purpose of committing any of the offences established in [relevant articles]; 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 [relevant articles]. 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 [relevant articles], 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.

Criminalization of cyberextortion

1. New Zealand would support the inclusion of a provision that criminalizes:

(a) The extortion of a user of a computer system to unlock data;

(b) The extortion of a user of a computer system with threats of the unauthorized release of data or personal information.

2. New Zealand looks forward to working with colleagues to develop precise language for this offending.

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.

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 are directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Sexual exploitation of children using computer systems

1. We look forward to working with colleagues to develop effective and comprehensive criminalization provisions relating to combating online sexual exploitation and abuse of children.

2. At a minimum, such offending should include offences relating to the use of a computer system to:

(a) Produce child sexual exploitation material;

(b) Offer or make available child sexual exploitation material;

(c) Distribute or transmit child sexual exploitation material;

(d) Procure child sexual exploitation material for oneself or for another person;

(e) Possess child sexual exploitation material;

(f) Groom children for the purposes of sexual exploitation.

Posting or distributing an intimate visual recording without consent

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law the transfer, sending, publishing, disseminating or otherwise communicating, by means of a computer system, without reasonable excuse, an intimate visual recording of a victim—

(a) Knowing that the victim has not consented to the posting; or

(b) Being reckless as to whether the victim has consented to the posting.

2. For clarity, a child or young person under the age of 16 years cannot consent to the posting of an intimate visual recording of which they are the subject.

Participation and attempt

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

Liability of legal persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this 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.

5. 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.

Criminalization of 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, knowing that such property is the proceeds of cybercrime, 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 cybercrime;

(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 cybercrime;

(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 crimes established in relevant article of this Convention and] the offences established in accordance with [relevant articles] of 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 when 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;

(f) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.

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.

Norway

[Original: English]
[8 April 2022]

Criminalization

4. We should suggest that the convention criminalizes offences that are cyber-dependent. Even though cybercrime develops every day, national and international agencies have managed to identify central reoccurring types of conduct. These offences are already criminalized in many Member States today. In that regard, the Government of the Kingdom of Norway would like to recommend that at least the following cyber-dependent offences be considered:

- Illegal access, i.e. accessing a computer or computer system without authorization
- Illegal interception, i.e. real-time unlawful interception of the content of communications or traffic data related to communications
- Data or system interference, i.e. malware, denial of service attacks, ransomware, data deletion or modification

- Misuse of devices, i.e. trafficking or using credit data, passwords and personal information which permit access to resources

2. We would like to keep the list short.

3. The convention should also avoid duplicating offences that are addressed in other legal instruments.

4. The text should be technology-neutral.

5. In addition to the short list of cyber-dependent crimes, the convention should include provisions on offences related to child sexual abuse materials.

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

[Original: Russian]
[7 April 2022]

Chapter II
Criminalization, criminal proceedings and law enforcement

Section 1
Establishment of liability

Article 5
Establishment of liability

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

Article 6
Unlawful access to digital information

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

Article 7
Unlawful interception

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

Article 8
Unlawful interference with digital information

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

Article 9
Disruption of information and communications networks

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

Article 10
Creation, utilization and distribution of malicious software

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

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

Article 11
Unlawful interference with critical information infrastructure

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

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

Article 12
Unauthorized access to personal data

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

Article 13
Illegal trafficking in devices

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the illegal manufacture, sale, purchase for use, import, export or other form of transfer for use of devices designed or adapted primarily for the purpose of committing any of the offences established under articles 6–12 of this Convention.

The provisions of this article shall not apply when the manufacture, sale, purchase for use, import, export or other form of transfer for use of devices is related, for example, to an authorized trial or to protection of a computer system.

Article 14
information and communications technology-related theft

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

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

Article 15
information and communications technology-related offences connected with the production and distribution of materials or objects with pornographic images of minors

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

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

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

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

(d) Using information and communications technologies to procure child pornography for oneself or for another person;

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

2. For the purposes of paragraph 1 of this article, the term “child pornography” shall include pornographic material that visually depicts:

(a) A minor engaged in sexually explicit conduct;

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

(c) Realistic images representing a minor engaged in sexually explicit conduct.

For the purposes of this article, the term “minor” shall include all persons under 18 years of age. A party may, however, require a lower age limit, which shall be not less than 16 years.

Article 16
Encouragement of or coercion to suicide

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

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

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

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

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

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

Article 19
Incitement to subversive or armed activity

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

Article 20
Crimes related to terrorist activity

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

Article 21
Extremism-related offences

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

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

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

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

Article 23
Offences related to arms trafficking

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

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

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

Article 25
Illicit distribution of counterfeit medicines and medical products

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

Article 26
Use of information and communications technologies to commit acts established as offences under international law

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the use of information and communications technologies for the purpose of committing an act constituting an offence under any of the international agreements listed in the Annex [36] to this Convention.

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

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

Article 27
Infringement of copyright and related rights by means of information and communications technologies

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the infringement of copyright and related rights, as defined by the legislation of that State party, when such acts are intentionally committed by means of information and communications technologies, including the illegal use of software for copyrighted computer systems or databases and appropriation of authorship.

[36] Note by the Secretariat: please refer to the annex in A/75/980.

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

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

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

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

Article 29
Other illegal acts

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

Article 30
Liability of legal persons

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

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

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

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

2. In addition to the cases provided for in paragraph 1 of this article, each State party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence or other illegal act established as such under this Convention for the benefit of that legal person by a natural person acting under its authority.

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

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

South Africa

[Original: English]
[14 April 2022]

Chapter II. Criminalization

Article 5: Illegal access

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 unlawfully, the illegal 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 unlawfully obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 6: 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 and unlawfully, 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 7: Unauthorized interference with digital information

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 unlawfully, 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 (to natural persons, juristic persons and the economy of a State Party).

Article 8: System interference and disruption of information and communication networks

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 unlawfully, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 9: Creation, utilization and distribution of devices

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 unlawfully 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 5 through 26;

(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 5 through 26; and

(b) The possession of an item referred to in paragraph 1 (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in articles 5 through 26. 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 5 through 26 of this Convention, such as for the authorized testing or protection of a computer system.

3. Each State 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 10: Cyber-enabled forgery

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 unlawfully 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 are directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 11: Cyber-enabled fraud

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 unlawfully 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 12: Offences related to child sexual abuse materials

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 unlawfully, the following conduct:

(a) Producing child sexual abuse materials for the purpose of its distribution through a computer system or information and communications technologies;

(b) Offering or making available child sexual abuse materials through a computer system or information and communications technologies;

(c) Distributing or transmitting child sexual abuse materials through a computer system or information and communications technologies;

(d) Procuring child sexual abuse materials through a computer system or information and communications technologies for oneself or for another person;

(e) Possessing child sexual abuse materials in a computer system or information and communications technologies or on a computer data storage medium.

2. For the purpose of paragraph 1 above, the term “child sexual abuse materials” shall include 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; and

(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.

Article 13: Offences related to infringements of copyright and related rights

1. Each State 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 various international treaties and agreements, 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 or information and communications technologies.

2. Each State 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 or information and communications technologies.

3. A State 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 14: 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 a criminal offence under its domestic law acts, involving the use of information and communications technologies, that further the trafficking in narcotic drugs, psychotropic substances and materials required for their manufacture.

Article 15: Protection of reporting persons

Each State Party shall consider incorporating into its domestic legal system appropriate measures to provide protection against any unjustified treatment for any person who reports in good faith and on reasonable grounds to the competent authorities any facts concerning offences involving the use of information and communications technologies established in accordance with this Convention.

Each State Party shall consider incorporating into its domestic legislation indemnity from prosecution, subject to satisfying standards/conditions adopted by a Party, of anyone providing full cooperation and in good faith when interacting with relevant law enforcement agencies.

Article 16: Cooperation with law enforcement authorities

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in the commission of an offence involving the use of information and communications technologies established in accordance with this Convention to supply information in good faith which is useful to competent authorities for investigative and evidentiary purposes and to provide factual, specific help to competent authorities that may contribute to depriving offenders of the proceeds of crime and to recovering such proceeds.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides, in good faith, substantial cooperation in the investigation and prosecution of an offence involving the use of information and communications technologies 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, in good faith, substantial cooperation in the investigation or prosecution of an offence involving the use of information and communications technologies established in accordance with this Convention.

4. Protection of such persons shall be, mutatis mutandis, as provided for in article 22 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.

6. Each State Party shall maintain a register with identifiable information of all domain name registrars, crypto asset traders and crypto assets within its jurisdiction, in accordance with fundamental principles of its domestic law, and supply such information to competent authorities for investigative and evidentiary purpose.

Article 17: Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences involving the use of information and communications technologies established in accordance with this Convention when:

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

(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 involving the use of information and communications technologies when:

(a) The offence is committed against a national of that State Party; or

(b) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory; or

(c) The offence is one of those established in accordance with article 17, paragraph 1 (b)(ii), of this Convention and is committed outside its territory with a view to the commission of an offence involving the use of information and communications technologies established in accordance with article 15 of this Convention within its territory; or

(d) The offence is committed against the State Party or has direct impact on the affairs of such State Party.

3. For the purposes of article [on Extradition] of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences involving the use of information and communications technologies 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 involving the use of information and communications technologies 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.

Switzerland

[Original: English]
[8 April 2022]

2.2 Provisions on criminalization

a. Offences against the confidentiality, integrity and availability of computer data and systems

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.

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.

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.

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.

Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(a) The production, sale, procurement for use, import, distribution or otherwise making available of:

(i) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the provisions on illegal access, illegal interception, data interference or system interference of this Convention;

(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 the provisions on illegal access, illegal interception, data interference or system interference of this Convention; and

(b) The possession of an item referred to in paragraph 1 (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in accordance with the provisions on illegal access, illegal interception, data interference or system interference of this Convention. A Party may require 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 the provisions on illegal access, illegal interception, data interference or system interference 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.

b. Computer-related offences

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 are directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

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.

c. Content-related offences

Offences related to child sexual exploitation and abuse material

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 sexual exploitation and abuse material for the purpose of its distribution through a computer system;

(b) Offering or making available child sexual exploitation and abuse material through a computer system;

(c) Distributing or transmitting child sexual exploitation and abuse material through a computer system;

(d) Procuring child sexual exploitation and abuse material through a computer system for oneself or for another person;

(e) Possessing child sexual exploitation and abuse material in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term "child sexual exploitation and abuse material" shall include 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, paragraph 1, subparagraphs (d) and €, and paragraph 2, subparagraphs (b) and (c).

d. Ancillary liability and sanctions

Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with the provisions on criminalization of this Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with the provisions on criminalization of this Convention.

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

Liability of legal persons

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with the provisions on criminalization of this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

(a) A power of representation of the legal person;

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

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

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

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

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

Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with the provisions on criminalization of this Convention are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with the provision on liability of legal persons of this Convention shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[12 April 2022]

Chapter – Criminalization

Cyber-dependent offences

The United Kingdom believes the Convention must include cyber-dependent offences with descriptions and definitions that are acceptable to all parties, and which are consistent with existing international agreements in this area.

Article 5
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 6
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 7
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 8
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 9
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 sections;

(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 the other four Articles in this section; and

(b) the possession of an item referred to in paragraph 1 (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in the other four Articles in this section. 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 relating to illegal

access, illegal interception, data interference and system interference, 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.

Cyber-enabled offences

The United Kingdom also believes cyber-enabled offences should be included where the offence is mainly carried out online, where computers change the scale and speed of the offence, and where the definitions of the offence are commonly understood.

Article 10
Fraud

Each party shall adopt such legislative changes and other measures as may be necessary to establish as a criminal offence under its domestic law the general offence of fraud committed in whole or partly online. This includes but is not limited to activity committed domestically, and across borders through the Internet, or other cyber-dependent/digital means by the following methods:

(a) Fraud by false representation;

(b) Fraud by failing to disclose information;

(c) Fraud by abuse of position, with fraudulent or dishonest intent to cause a loss to another or make a gain in money or other property for another person.

Article 11
Offences related to online child sexual exploitation and abuse, including child sexual exploitation and abuse material and online grooming

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 sexual exploitation and abuse material for the purpose of its distribution through a computer system;

(b) Offering or making available child sexual exploitation and abuse material through a computer system;

(c) Distributing or transmitting child sexual exploitation and abuse material through a computer system;

(d) Procuring child sexual exploitation and abuse material through a computer system for oneself or for another person;

(e) Possessing child sexual exploitation and abuse material in a computer system or on a computer data storage medium;

(f) Viewing child sexual exploitation and abuse material in a computer system or on a computer data storage.

2. For the purpose of paragraph 1 above, the term “child sexual exploitation and abuse material” shall include material that visually depicts:

(a) A minor engaged in real or simulated sexually explicit conduct;

(b) A person appearing to be a minor engaged in real or simulated sexually explicit conduct;

(c) Realistic images representing a minor engaged in real or simulated sexually explicit conduct;

(d) Any depiction of a minor's sexual organs for primarily sexual purposes.

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, paragraph 1, subparagraphs (d) and (e), and paragraph 2, subparagraphs (b) and (c).

Article 12
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 relating to the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the World Intellectual Property Organization (WIPO) Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (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 13
Attempts, aiding and abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with [this Convention] with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with this Convention.

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

Article 14
Prosecution, adjudication and sanctions

1. Each 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 Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by 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.

3. In the case of offences established in accordance with this Convention, each Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the 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.

4. Each Party shall ensure that its courts or other competent authorities bear in mind the grave nature of the offences covered by this Convention when considering the eventuality of early release or parole of persons convicted of such offences.

5. Each Party shall, where appropriate, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence covered by this Convention and a longer period where the alleged offender has evaded the administration of justice.

6. 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 Party and that such offences shall be prosecuted and punished in accordance with that law.

Article 15
Jurisdiction

1. Each Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when:

(a) The offence is committed in the territory of that Party; or

(b) The offence is committed on board a vessel that is flying the flag of that Party or an aircraft that is registered under the laws of that Party at the time that the offence is committed.

2. Subject to the relevant articles of this Convention, a Party may also establish its jurisdiction over any such offence when:

(a) The offence is committed against a national of that Party; or

(b) The offence is committed by a national of that Party or a stateless person who has his or her habitual residence in its territory; or

(c) The offence is committed against the Party.

3. For the purposes of any article in this Convention relating to extradition, each Party may 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 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 Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those 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 Party in accordance with its domestic law.

Additional comments

The United Kingdom believes that the use of digital technology to communicate with a minor where that communication is sexual in nature, or is made with the intention of encouraging the minor to engage in sexual communication or activity, and where that communication is made for the purpose of obtaining sexual gratification, should be criminalized, and we will provide text on this during negotiations.

The trafficking and sexual exploitation of women and girls is a particularly high-harm crime, and victims experience a multitude of abuses during the period of their exploitation that causes very high physical and emotional harm. As much of this exploitation is arranged and facilitated online, this is a global issue and the United Kingdom believes that we need a united approach to this threat. The United Kingdom supports including a provision in this Convention to criminalize modern slavery and human trafficking, including the trafficking and sexual exploitation through Adult Services Websites (ASWs).

The United Kingdom believes that the harm posed by the unauthorized sharing of intimate images requires us to take a coordinated approach to prevent such abuse, including through the removal of such images and through ensuring that there are effective penalties for those who share unauthorized images. The United Kingdom United Kingdom would like to include provisions to tackle this harm.

United Republic of Tanzania

[Original: English]
[11 April 2022]

4. Criminalization

Recently, there has been an exponential increase in the use of information and communications technologies for criminal purposes by groups of criminals worldwide due to technological development.

4.1 List of offences

Owing to this challenge, the United Republic of Tanzania sees the need for each State Party to adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed wilfully and intentionally, the following actions but not limited to:

(a) Illegal access;

(b) Illegal interception;

(c) Illegal destruction of electronic data and computer system;

(d) Data espionage;

(e) Illegal system interference;

(f) Owning illegal devices and/or software for purposes of committing crimes;

(g) Computer-related forgery and fraud;

(h) Pornography and child pornography;

(i) Identity-related crimes;

(j) Publication of false information;

(k) Racist and xenophobic materials;

(l) Genocide and crimes against humanity;

(m) Cyberbullying;

(n) Attempt, aiding and abetting;

(o) Participation in an organized criminal group.

4.2 Corporate liability

The United Republic of Tanzania proposes that the convention should require Member States to include, in their domestic legislations, the provisions that impose liability to the legal persons in relation to offences established by the Convention. The liability may extend to natural persons acting on behalf of, or under the cover of the corporate.

United States of America

[Original: English]
[8 April 2022]

Criminalization

Criminalization of cybercrimes

"Illegal access"

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the access to the whole or any part of a computer system without right. A State 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.

"Illegal interception"

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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 State 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.

"Data interference"

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

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

"System interference"

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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.

"Misuse of devices"

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right:

(a) The production, sale, procurement for use, import, distribution or otherwise making available of:

(i) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the preceding articles of this chapter;

(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 the intent that it be used for the purpose of committing any of the offences established in the preceding articles of this chapter; and

(b) The possession of an item referred to in paragraph 1 (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in the preceding articles of this chapter. A State 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 the preceding articles of this chapter, such as for the authorized testing or protection of a computer system.

3. Each State 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.

"Computer-related forgery"

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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 are directly readable or intelligible. A State Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

"Computer-related fraud"

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, 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.

"Computer-related offences involving child sexual abuse materials"

1. Each State Party shall take the necessary legislative or other measures to ensure that the following conduct, when committed knowingly and through a computer system, is criminalized:

(a) Producing child sexual abuse material;

(b) Causing the live transmission of a child engaged in sexually explicit conduct;

(c) Offering or making available child sexual abuse material;

(d) Distributing or transmitting child sexual abuse material;

(e) Procuring child sexual abuse material for oneself or for another person;

(f) Possessing child sexual abuse material;

(g) Knowingly obtaining access, through information and communication technologies, to child sexual abuse material or viewing the live transmission of a child engaged in sexually explicit conduct.

2. Each State Party shall take the necessary legislative or other measures to criminalize the knowing persuasion, inducement, enticement or coercion, through information and communication technologies, of a child, or an individual believed to be a child, to engage in any illegal sexual activity. Each State Party shall take such necessary legislative or other measures to assure that its national law does not require a meeting in person between the individual and a child.

"Computer-related offences related to infringements of copyright and related rights"

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences the infringement of copyright, as defined under the law of that State Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 relating to the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the World Intellectual Property Organization (WIPO) Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each State 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 Organizations (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 State 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.

"Participation and attempt"[37]

1. Each State Party shall adopt such legislative and other measures as may be necessary 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.

[37] United Nations Convention against Corruption, article 27.

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

Liability of legal persons[38]

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for the offences established in accordance with the criminalization articles of this 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.

Prosecution, adjudication and sanctions[39]

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

2. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by 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.

3. In the case of offences established in accordance with the criminalization articles of this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the 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.

4. Each State Party shall ensure that its courts or other competent authorities bear in mind the grave nature of the offences covered by this Convention when considering the eventuality of early release or parole of persons convicted of such offences.

5. 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 covered by this Convention and a longer period where the alleged offender has evaded the administration of justice.

6. 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 the 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.

[38] United Nations Convention against Transnational Organized Crime, article 10, and United Nations Convention against Corruption, article 26.

[39] United Nations Convention against Transnational Organized Crime, article 11.

Criminalization of the laundering of proceeds of cybercrime[40]

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, 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 include as predicate offences the offences established in accordance with the criminalization articles of this Convention. In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include the offences that are set forth in this Convention;

(b) 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 when 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;

(c) 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;

(d) 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;

(e) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.

Criminalization of obstruction of justice[41]

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

[40] Adapted from article 6 of the United Nations Convention against Transnational Organized Crime.
[41] United Nations Convention against Transnational Organized Crime, article 23.

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.

Venezuela (Bolivarian Republic of)

[Original: Spanish]
[13 April 2022]

5. Criminalization

The convention would oblige States parties to establish criminal and other offences in order to cover a wide range of illicit acts relating to the use of information and communications technologies where the acts defined in the convention do not already constitute crimes under domestic law. In some cases, States would have a legal obligation to establish offences, while in others, in order to take into account differences in national legislation, they would be obliged to elaborate relevant legislation.

Accordingly, criminal activities that are perpetrated using information and communications technologies and are widely recognized in the international community must be clearly defined. The convention should provide a forward-looking framework with a view to coordinating criminalization, meeting current and future information and communications technology development needs and combating crime.

In the light of the above, each State party should adopt such legislative, policy and other measures as may be necessary to establish the offences in question. The convention should therefore contain provisions ensuring that States that need to adapt their national legislation and programmes have time to do so and receive the necessary support.

The principal offences to be covered by the convention should include the following:

- Access without due authorization to digital information where such access has led to the destruction, blocking or modification of that information
- The premeditated interception of digital information without appropriate authorization and/or in violation of established rules, including through the use of technical means to intercept traffic data and data not intended for public use that are processed by means of information and communications technologies
- The unlawful manipulation of digital information by damaging, deleting, altering, blocking or modifying it
- Premeditated unlawful acts intended to cause a malfunction of information and communications networks that entails or poses the risk of serious consequences
- The use and distribution of malicious software intended for the unauthorized destruction, blocking, modification or dissemination of digital information or for the neutralization of security features
- The intentional and premeditated creation, distribution and/or use of software or other digital information for the purpose of unlawful manipulation of critical information infrastructure, including for the destruction, blocking or modification of information contained therein or the neutralization of security features
- The intentional creation, distribution and/or use of software or other digital information knowingly designed to interfere unlawfully with critical information infrastructure, including software or other digital information for

the destruction, blocking, modification or copying of information contained therein, or for the neutralization of security features

- Violation of the rules of operation of the means used to store, process and transmit protected digital information contained in critical information infrastructure, or of information systems or information and communications networks belonging to critical information infrastructure, or violation of the rules of access to them, if such violation damages the critical information infrastructure
- The theft of property or the illegal acquisition of rights over property, including by means of fraud through the destruction, blocking or modification of digital information or other interference with information and communications technologies operations
- Calls issued by means of information and communications technologies for subversive or armed activities directed towards the violent overthrow of the Government of another State
- Calls issued by means of information and communications technologies for the incitement of, recruitment for the purposes of or other involvement in terrorist activities, for advocacy and justification of terrorism, or for the collection or provision of funds for its financing
- Trafficking in narcotic drugs and psychotropic substances and in materials required for their manufacture, by means of information and communications technologies
- Trafficking in arms, ammunition, explosive devices and explosive substances by means of information and communications technologies
- Unauthorized access to personal data in order to destroy, modify, copy or share it
- Information and communications technology-related offences connected with the production and distribution of materials or objects with pornographic images of minors
- Offences related to the involvement of minors in the commission of illegal acts that endanger their life or health

Viet Nam

[Original: English]
[12 April 2022]

Chapter II. Criminalization

5. Each Member State shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed unauthorizedly and intentionally:

(a) To manufacture, trade, transfer instruments, equipment or software meant to attack a computer network, telecommunications network or an electronic device which to be used for criminal activities as governed in this Convention;

(b) To spread a software program that is harmful to a computer network, telecommunications network or an electronic device;

(c) To delete, sabotage or modify a software program or digital data;

(d) To obstruct the transmission of data of a computer network, telecommunications network or an electronic device;

(e) To obstruct or disturb normal operations of a computer network, telecommunications network or an electronic device;

(f) To take control or interfere in the operation of an electronic device by bypassing security or protection system, abusing the rights of administration of another person, or any other means;

(g) To steal, modify, sabotage or counterfeit information or data;

(h) To uses a computer network, telecommunications network or electronic device for the following purposes:

(i) Using information of bank account or bank card of an organization or an individual to illegally appropriate assets;

(ii) Manufacturing, possessing, trading or using counterfeit bank card in order to illegally appropriate assets;

(iii) Unauthorized accessing accounts of government agencies, organizations and individuals for illegal appropriation of assets;

(iv) To commit frauds in e-commerce, electronic payment, online currency trading, online capital rising, online multilevel marketing or online securities trading for the purpose of property appropriation;

(v) Unauthorized establishing or providing telecommunication or Internet service for the purpose of property appropriation;

(i) To collect, possess, trade, transfer or publicize information of bank account of individuals and organizations.

(j) To trade, transfer, modify, publicize private information of government agencies, organizations or individuals without a consent of the owners.

(k) o use cyberspace, information technologies or electronic devices to undertake an act of terrorism or terrorist financing.

6. Nothing in this Convention shall prevent Member States from adopting such legislative and other measures as may be necessary to establish as criminal offences of any other act involving the use of information and communications technologies for criminal purposes.

7. 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 Member State and that such offences shall be prosecuted and punished in accordance with that law.