United Nations A/AC.291/9/Add.3

General Assembly

Distr.: General
16 May 2022

Original: English

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

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

Addendum

Contents

V.22-03011 (E) 240522 250522

V. Additional submissions

Introduction

This addendum contains submissions from Member States 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 received after 14 April 2022; the submissions are not organized into thematic chapters.

India

[Original: English]
[12 May 2022]

Background

1. Cyberspace, being a complex environment of people, software, hardware and services on the Internet, has distinct and unique characteristics as compared to physical space. The cyberspace is virtual, borderless and offers anonymity. In recent years, social media and the mobile ecosystem have emerged as one of the important public communication channels. Of late, use of social media has been seen all over the world as a key tool used by criminals and anti-national elements to commit cybercrime. With a borderless cyberspace coupled with the possibility of instant communication and anonymity, the potential for committing cybercrime through the use of social media and the Internet is higher than ever in the country, like elsewhere in the world.

2. Cybercrime has also become a major issue while there is an upsurge in usage of information and communication technology devices globally. The advancement of technology has made humans dependent on information and communication technologies for all their requirements. Unlike conventional crime, cybercrime has no geographical boundaries, and the cybercriminals are unknown and even anonymous, which affects all stakeholders, including common citizens. The following section emphasizes the types of cybercrimes that occur globally.

Classification of crimes committed through the use of information and communication technologies

3. Cybercrime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target or a place of criminal activity and includes everything from electronic wrecking to denial-of-service attacks. In general, cybercrime can be classified as “cyber-enabled crime” [1] and “cyber-dependent crime”.[2] Further, cybercrime can also be classified as “cybercrimes against persons”, “cybercrimes against property” and “cybercrimes against government”. However, it may be better to use the definition of “crimes committed through the use of information and communications technologies” as it will be able to cover new and emerging technologies as well.

Criminalization

4. Each State party shall adopt such legislative and other measures as are necessary, as provided in the following points, to establish as an offence or its equivalent clauses under its domestic law. (The list given below is indicative and more

[1] Such as theft, harassment, child exploitation, fraud and scams that can be committed without a computer but are enabled by a computer in certain circumstances.

[2] Hacking, ransomware, distributed denial-of-service attacks and malware, distribution of a virus and cyberterrorism.

crimes may be added that are committed through the use of information and communication technologies.)

4(a) Damage to a computer, computer system, etc.

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network:

(a) Accesses or secures access to such computer, computer system or computer network or computer resource;

(b) Downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network, including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act or rules or regulations made thereunder;

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network;

(i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) Steals, conceals, destroys or alters, or causes any person to steal, conceal, destroy or alter, any computer source code used for a computer resource with an intention to cause damage.

4(b) Failure to protect data

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person.

4(c) Tampering with computer source documents

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, when any person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable.

4(d) Sending offensive messages through communication service, etc.

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person sends, by means of a computer resource or a communication device:

(a) Any information that is grossly offensive or has a menacing character;

(b) Any information which he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently, by making use of such a computer resource or a communication device;

(c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

4(e) Dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device.

4(f) Identity theft (impersonation)

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person.

4(g) Cheating by personation by using computer resource (impersonation)

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person, by means of any communication device or computer resource cheats by impersonation.

4(h) Violation of privacy

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person, intentionally or knowingly, captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person:

(a) “Transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “Capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “Private area” means the naked or undergarment-clad genitals, public area, buttocks or female breast;

(d) “Publishes” means reproduction in printed or electronic form and making it available for public;

(e) “Under circumstances violating privacy” means under circumstances in which a person can have a reasonable expectation that:

(i) He or she could disrobe in privacy without being concerned that an image of his or her private area was being captured; or

(ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

4(i) Cyberterrorism

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person:

(a) With the intent to threaten the unity, integrity, security or sovereignty of State or to strike terror in the people or any section of the people by:

(i) Denying or causing the denial of access to any person authorized to access a computer resource; or

(ii) Attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) Introducing or causing to introduce any computer contaminant;

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure; or

(b) Knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or a computer database that is restricted for reasons of the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of State, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyberterrorism.

2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the commission or conspiracy to commit the offence as described in paragraph 1 (a) and (b).

4(j) Publishing or transmitting obscene material in electronic form communications

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person, publishes or transmits or causes to be published or transmitted in electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

4(k) Publishing or transmitting of material containing sexually explicit act, etc., in electronic form

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person, publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct.

4(l) Publishing or transmitting of material depicting children in a sexually explicit act, etc., in electronic form

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law, if any person:

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) Facilitates abusing children online; or

(e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children;

provided this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form:

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) Which is kept or used for bona fide heritage or religious purposes.

The age of "children" is as defined in the domestic legislation of that State.

4(m) Disclosure of information in breach of lawful contract

Save as otherwise provided in this Convention, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person.

5. Other unlawful acts committed using information and communication technologies

Without prejudice to (article on protection of sovereignty) the Contracting Parties shall mutually agree on any other unlawful acts committed using information and communication technologies for the purpose of cooperation established under this Convention. (There should be a provision in this Convention entitled "Other unlawful acts" considering the advancement in information and communication technologies). In addition, the following cybercrimes may be further extended, as criminalization mentioned in the United Nations Office on Drugs and Crime document,[3] through this Convention:

- Illegal access
- Illegal interception: interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic illegal interference
- Computer misuse tools
- Identity offences
- Personal harm
- Racism and xenophobia
- Terrorism support offences
- Ransomware

[3] Source: United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, draft of February 2013, p. 22.

13. Terms of usage

(a) “Communication device” means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;

(b) “Computer” means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

(c) “Computer network” means the interconnection of one or more computers or computer systems or communication device through:

(i) The use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) Terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

(d) “Computer resource” means computer, computer system, computer network, data, computer database or software;

(e) “Computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(f) “Computer contaminant” means any set of computer instructions that are designed:

(i) To modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(ii) By any means to usurp the normal operation of the computer, computer system or computer network;

(g) “Computer database” means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(h) “Computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(i) “Damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means;

(j) “Computer source code” means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form;

(k) “Cybersecurity” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction;

(l) “Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized

manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network or cloud, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(m) “Information” includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer-generated microfiche;

(n) “Body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(o) “Reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the States parties in consultation with such professional bodies or associations as it may deem fit;

(p) “Sensitive personal data or information” means such personal information as may be prescribed by the States parties in consultation with such professional bodies or associations as it may deem fit;

(q) “Electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record which may be transmitted with the message;

(r) “Social media intermediary” means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;

(s) “Electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche;

(t) “Originator” means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

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

(v) “Proceeds of crime” means any property derived from or obtained, directly or indirectly, through the commission of an offence or other unlawful act as established under this Convention;

(w) “Confiscation” includes forfeiture where applicable and shall mean the permanent deprivation of property by order of a court or other competent authority;

(x) “Predicate offence” shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in this Convention;

(y) “Child pornography” means any representation, by whatever means, or a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

14. Data-oriented Jurisdiction

Data-oriented jurisdiction means that the country whose citizen's data are being stored/processed/screened/federated anywhere in the world should be having the broader jurisdiction of the data immaterial of where the data are physically stored/processed/screened/federated. This data-oriented jurisdiction will ensure the primality of data ownership and the issue of privacy (an acknowledged fundamental right of a global citizen) and human rights.

(*Brief explanation: In the current day scenario, the classical Westphalian model-based jurisdiction does not hold good in cyberspace, especially involving cloud resources that result in a jurisdictional nightmare. An example of a typical scenario may involve a cybercrime executed involving the processing power in the cloud originating in one country and the storage aggregation in another country, with the cloud service provider registered in a third country, and the user (the victim and the attacker) whose data are being held by the service provider may be the resident of a fourth country. Clearly in such a situation, it is extremely difficult to ascertain jurisdiction based on the classical territorial models. In view of the above, India proposes that rather than a territorial-based jurisdictional model, the Convention adopt a data-oriented jurisdiction. The data ownership which is linked to privacy is an acknowledged fundamental right of a global citizen. This has been acknowledged by the European Court of Justice, whereby it recognized the individual's right to be forgotten. The right to privacy is also linked to human rights, which has been raised by large number of countries in the Ad Hoc Committee, and the data-oriented jurisdiction will help protect the right to privacy, fundamental rights and human rights.*)

15. "Jurisdiction" may be defined as follows

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

(a) The offence is committed in the territory of that State Party or having a bearing in the territory of the 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 this Convention, a State Party may also establish its jurisdiction over any such offence when:

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

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

(c) The offence is committed outside its territory with a view to the commission of an offence established in accordance with this Convention within its territory;

(d) The offence is committed against the State Party; or

(e) The offence is committed targeting computer resources located within its territory;

(f) The offence involves the digital/electronic data of their nationals, irrespective of the place of its physical storage/processing/screening/federation.

3. For the purposes of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution, or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions. For the purpose of consultation under this article, the Contracting Parties shall take into account the data-oriented jurisdiction, i.e. data belonging to the victim of the cybercrime or unlawful act committed using information and communication technologies.

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.

17. Search and seizure of information stored or processed electronically

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

(a) A computer system or part of it and computer data stored therein; and

(b) A computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a) and have grounds to believe that the data sought are stored in another computer system or part of it in its territory, and such data are lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

(a) Seize or similarly secure a computer system or part of it or a computer-data storage medium;

(b) Make and retain a copy of those computer data;

(c) To preserve/maintain integrity of the computer data.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

18. Real-time collection of traffic data

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

(a) Collect or record through the application of technical means on the territory of that Party; and

(b) Compel a service provider, within its existing technical capability:

(i) To collect or record through the application of technical means on the territory of that Party; or

(ii) To cooperate and assist the competent authorities in the collection or recording of traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

19. Collection of content and metadata

1. Each Party shall adopt such legislative and other measures as may be necessary to provide metadata expeditiously without the need of mutual legal assistance treaties. The service provider that has such metadata shall provide such information on direct request of the law enforcement agencies through the designated nodal agency of each State.

2. Each Party shall adopt such legislative and other measures as may be necessary to provide content data expeditiously. The mechanism for such expeditious data-sharing will be developed under this Convention.

20. Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

(a) Collect or record through the application of technical means on the territory of that Party; and

(b) Compel a service provider, within its existing technical capability:

(i) To collect or record through the application of technical means on the territory of that Party; or

(ii) To cooperate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

21. Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic and content data, that have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige

that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 180 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. Each party shall create a nodal point for coordination by which such request for preservation can be carried out by the other state.

Jamaica (on behalf of the Caribbean Community)

[Original: English]
[12 May 2022]

Chapter 1. General provisions

Article. General provisions

The purposes of this Convention are as follows:

1. To promote and strengthen measures aimed at preventing and combating crimes and other unlawful actions directed against the confidentiality, integrity and availability of information and communication technology systems and computer data more efficiently and effectively.

2. To promote, facilitate and support international cooperation and technical assistance to prevent and combat criminal offences and other unlawful actions directed against the confidentiality, integrity and availability of information and communication technology systems and computer data.

3. To promote, facilitate and support international cooperation and technical assistance in the recovery of assets resulting from criminal offences and other unlawful actions referred to in this Convention.

Article. Scope of application

1. In accordance with its provisions, this Convention shall apply to the prevention, investigation and prosecution of criminal offences, to the promotion, facilitation and support of international cooperation in preventing and combating the use of information and communications technologies for criminal offences, and to the freezing, seizure, confiscation and return of the proceeds of such offences established in accordance with this Convention.

2. For the purposes of implementing this Convention, it shall not be necessary, except as otherwise stated therein, for the criminal offences established pursuant to its provisions to result in damage or harm to persons, property and the State.

Article. Protection of sovereignty

1. States parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereignty, sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States Parties or States.

2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State Party or State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State Party or State in accordance with its domestic law and in accordance with international law and obligations.

Chapter 2. Criminalization

Article. Illegal/unauthorized access to computer systems or data

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 access to the whole or any part of a computer system. A State Party may require that the offence is committed where there is a breach or infringement of a security measure or 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. *(Based on the Budapest Convention, article 2 – Illegal access)*

Article. Illegal/unauthorized interception

1. Each State Party shall adopt such legislative and other measures as are necessary to establish as a criminal offence, when committed intentionally, the interception without right or authority of a computer system or data, where such interception is done by technical means to intercept traffic data and data processed by means of information communication technology which is not intended for public use, 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. 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 inputting, damaging, deletion, deterioration, alteration or suppression of computer data without right or authority.

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

Article. Illegal system interference

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 or authority, the hindering of the functioning of an information and communication technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

2. Each State Party may reserve the right to impose an aggravation of penalty where the actions as outlined in paragraph 1 involve or affect critical infrastructure.

Article. Misuse of devices/malicious software/computer program

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 criminal offences established in accordance with articles (Unauthorized/illegal access, unauthorized/illegal interception/data interference/system interference);

(ii) A computer password, access code or similar data by which the whole or any part of an information, communication and technology system is capable of being accessed, with the intent that it be used for the purpose of committing any of the criminal offences established in articles (Unauthorized/illegal access, unauthorized/ illegal interception/data interference/system interference); and

(b) The possession of an item referred to in subparagraphs (a)(i) or (ii) above, with the intent that it be used for the purpose of committing any of the criminal offences established in articles (Unauthorized/illegal access, unauthorized/illegal interception/ data interference/system interference). 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 a criminal offence established in accordance with articles (Unauthorized/illegal access, unauthorized/illegal interception/data interference/ system interference) 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. Content-related offences

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, the following conduct:

(a) Producing child sexual exploitation and abuse material through an information and communication technology system;

(b) Offering or making available child sexual exploitation and abuse material through an information and communication technology system;

(c) Distributing or transmitting child sexual exploitation and abuse material through an information and communication technology system;

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

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

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

(a) A child engaged in sexually explicit conduct;

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

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

3. For the purposes of paragraph 2 above, the term “child” means every human being below the age of eighteen (18) years unless under the law applicable to the child, majority is attained earlier. (*Convention on the Rights of the Child, article 1*)

Article. Violation of privacy/non-consensual distribution of sexual images

1. Each State Party shall adopt such legislative and other measures as are necessary to establish as a criminal offence, when committed intentionally and without right, the following conduct:

(a) Knowingly publishing, distributing, transmitting, selling, making available or advertising an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct;

(b) The publishing, distributing, transmitting, selling, making available or advertising of an intimate image of a person is done with the intention to harass or cause harm to the person depicted in the image.

Definition of “intimate image”

2. In this article, “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 his or her genital organs or anal region or breasts, or the person is engaged in explicit sexual activity;

(b) In respect of which, at the time of recording, there were circumstances that gave rise to a reasonable expectation of privacy; and

(c) In respect of which the person depicted continues to have a reasonable expectation of privacy at the time the offence is committed.

Article. Intellectual property

Each State Party shall adopt such legislative and other measures as are necessary to establish as criminal offences the infringement of copyright and related rights, as defined by the legislation of the State Party, when such acts are wilfully committed by means of information and communication technology and on a commercial scale.

Computer-related offences

Article. Computer-related forgery

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, the input, alteration, deletion or suppression of computer data, resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible.

2. A State Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article. Computer-related fraud

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 or authority, the causing of a loss of property to another person by:

(a) Any input, alteration, erasure or suppression of computer data;

(b) 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.

Article. Inchoate offences

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences participation in any capacity such as an accomplice, assistant, instigator, abettor or conspirator 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 any attempt to commit an offence established in accordance with this Convention.

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

Article. 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 commission of a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as a part of an organ of the legal person, who holds a leading position within it, by virtue of:

(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 supervision or control within the legal person.

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

3. Subject to the domestic law of the State Party, the liability of legal persons may be criminal, civil or administrative.

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

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

Article. Sanctions and measures

1. Each State Party shall make the commission of a criminal offence established in accordance with this Convention liable to sanctions that are commensurate to the gravity of that offence, and are effective, proportionate and dissuasive, including the deprivation of liberty.

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

Chapter 3. Procedural law and law enforcement

Article. Scope of procedural provisions

1. Each State Party shall adopt legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of criminal investigations or proceedings.

2. Except as otherwise provided in article (Interception of communication), each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences established in accordance with articles (the criminalization provisions) of this Convention;

(b) Other criminal offences committed by means of an information, communication and technology system; and

(c) The collection of evidence in electronic form of a criminal offence.

3. Each State Party may reserve the right to apply the measures referred to in article (Real-time collection of data) only to criminal offences or categories of criminal offences specified in the reservation, provided that the range of such offences is not

more restricted than the range of criminal offences to which the State Party applies the measures referred to in article (Interception of content data).

4. Where a State Party, due to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in article (Real-time collection of data) and article (Interception of content data) to communications being transmitted within a computer system of a service provider, which system:

(i) Is being operated for the benefit of a closed group of users; and

(ii) Does not employ public communications networks and is not connected with another computer system, whether public or private;

that State Party may reserve the right not to apply those measures to such communications.

5. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in articles (Real-time collection of data and interception of content data).

Article. Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this article are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the International Covenant on Civil and Political Rights of 1966 and other applicable international human rights instruments.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application and the limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each State Party shall consider the impact of these powers and procedures in this article upon the rights, responsibilities and legitimate interests of third parties.

Article. Expedited preservation of computer data

1. Each State Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly expeditiously obtain, collect and preserve specified computer data, including traffic data, in particular where there are grounds for believing that the data are particularly vulnerable to deletion, modification or loss.

2. Where a State Party gives effect to paragraph 1 above by means of an order to a person, including to a legal person, to preserve specified stored computer data in the person's possession or control, the State Party shall adopt such legislative and other measures as may be necessary to require that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, but no longer than the period determined by the domestic law of that State Party, to enable the competent authorities to seek disclosure of the data. A State Party may provide for such an order to be subsequently renewed.

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

4. The powers and procedures referred to in this article shall be established in accordance with the articles (Scope of procedural provisions, and conditions and safeguards).

Article. Expedited preservation and partial disclosure of traffic data

1. Each State Party shall adopt, in respect of traffic data that are to be preserved under the article (Expedited preservation of computer data), such legislative and other measures as may be necessary to:

(a) Ensure that such expeditious preservation of traffic data are available regardless of whether one or more service providers are involved in the transmission of that communication; and

(b) Ensure the expeditious disclosure to the State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in this article shall be subject to articles (Scope of procedural provisions, and conditions and safeguards).

Article. Production order

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to order:

(a) A person, including to a legal person, in its territory to submit computer data in that person's possession or control, which are stored in a computer system or a computer-data storage medium; and

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

2. The powers and procedures referred to in this article shall be established in accordance with articles. (Scope of procedural provisions, and conditions and safeguards)

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

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

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

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

Article. Search and seizure of information stored or processed electronically

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to search or similarly access:

(a) An information and communication technology system or part of it and computer data stored therein; and

(b) A computer-data storage medium in which computer data may be stored in its territory.

2. Each State Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have reasonable grounds to believe that the data sought are stored in another computer system or part

of it in its territory, and such data are lawfully accessible from or available to the initial system, the authorities shall be able expeditiously to extend the search or similar accessing to the other system.

3. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

(a) Seize or similarly secure a computer system or part of it or a computer-data storage medium;

(b) Make and retain a copy of those computer data;

(c) Maintain the integrity of the relevant stored computer data;

(d) Render inaccessible or remove those computer data in the accessed computer system.

4. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1, 2 and 3.

5. The powers and procedures referred to in this article shall be subject to articles (Scope of procedural provisions, and conditions and safeguards).

Article. Real-time collection of traffic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to:

(a) Collect or record through the application of technical means in the territory of that Party; and

(b) Compel a service provider, within its existing technical capability:

(i) To collect or record through the application of technical means in the territory of that Party; or

(ii) To cooperate and assist the competent authorities in the collection or recording of traffic data, in real time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a State Party, in accordance with its domestic law, cannot adopt the measures referred to in paragraph 1(a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to require a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to articles (Scope of procedural provisions, and conditions and safeguards).

Article. Interception of content data

1. Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious criminal offences to be determined by domestic law, to empower its competent authorities, where there is reasonable belief that a criminal offence was committed or is being committed, to:

(a) Collect, record or store through the application of technical means in the territory of that Party, and

(b) Compel a service provider, within its existing technical capability:

(i) To collect, record or store through the application of technical means in the territory of that Party, or

(ii) To cooperate and assist the competent authorities in the collection or recording of content data, in real time, of specified communications in its territory transmitted by means of a computer system.

2. Where a State Party, in accordance with its domestic law, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to require a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to articles (Scope of procedural provisions, and conditions and safeguards).

Malaysia

[Original: English]
[20 April 2022]

Chapter I. General provisions

Article 1. Statement of purpose

The purposes of this Convention are:

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

(b) To promote and facilitate international cooperation;

(c) To support capacity building and technical assistance to enable Member States to strengthen their capacity to address cybercrime; and

(d) To ensure a proper balance between the interests of law enforcement and respect for fundamental human rights.

Article 2. Use of terms

For the purpose of this Convention:

(a) “Child” means any individual under the age of 18;

(b) “Competent authority” means a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorize or undertake the execution of measures under this Convention with respect to criminal investigations or proceedings;

(c) “Computer” means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand-held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

(d) “Cybercrimes” means offences established in accordance with this Convention;

(e) “Data” means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

(f) “Function” includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

(g) “Program” means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

Article 3. Scope of applications

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

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

3. The provision and conduct of technical assistance and capacity building on matters covered by this Convention.

Article 4. Protection of sovereignty

1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.

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

Chapter II. Criminalization and law enforcement

Article 5. Unauthorized access

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the unauthorized access of any kind by any person to any program or data held in a computer.

Article 6. Unauthorized interception

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the unauthorized interception of any kind by any person to any data or communications.

Article 7. Data interference

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, the damaging, deletion, deterioration or alteration 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.

Article 8. Obstruction of a computer, program or data

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the serious obstruction of a computer program or data by interfering with, interrupting, supressing, impeding, preventing access to or impairing.

Article 9. Misuse of data, program or computer

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 production, adaptation, sale, procurement for use, import, offer, distribution, supply or otherwise making available any data, program or computer.

Article 10. Offences related to child pornography

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

(a) Making, producing or directing the making of production of any child pornography for the purpose of its distribution through a computer system;

(b) Using, or causing to be used, a child in the preparation to make or produce, or in the preparation to direct the making or production of, or in the making or production of, or in the directing of the making or production of child pornography for the purpose of its distribution through a computer system;

(c) Exchanging, publishing, printing, reproducing, selling, letting for hire, distributing, exhibiting, advertising, transmitting, promoting, importing, exporting, conveying, offering or making available, through a computer system, any child pornography;

(d) Obtaining, collecting or seeking any child pornography through a computer system;

(e) Participating in or receiving profits from any business that the person knows or has reason to believe is related to any child pornography through a computer system;

(f) Accessing, or having in personal possession or control, any child pornography through a computer system.

2. For the purpose of paragraph 1, the term “child pornography” is 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.

Article 11. Attempt and aiding and abetting

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, abetting or 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.

Article 12. 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.

Article 13. Prosecution, adjudication and sanctions

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

2. Each State Party 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 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. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.

Chapter III. Criminal procedures and law enforcement

Article 14. Scope of procedural measures

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of criminal investigations or proceedings.

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

(a) The criminal offences established in accordance with the offences defined in this Convention;

(b) Other criminal offences committed by means of a computer system; and

(c) The collection of evidence in electronic form of a criminal offence.

Article 15. Production order

Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory to submit specified computer data in that person’s possession or control, which are stored in a computer system or a computer-data storage medium.

Article 16. Search and seizure of stored computer data

Each State Party shall adopt measures as may be necessary to empower its competent authorities to search for, seize and detain any such evidence, and the competent authorities shall be entitled to any program or data held in any computer or have access to, inspect or check the operation of, any computer and any associated apparatus or material which the competent authorities have reasonable cause to suspect is or has been in use in connection with any offence under this Convention.

Article 17. Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over offences 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 the sovereignty article of this Convention, 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; or

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

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

3. For the purposes of the extradition article of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution, or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

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

Article 18. Rights of victims

1. Each State Party shall establish appropriate procedures to provide access to compensation for victims of offences covered by this Convention.

2. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

Singapore

[Original: English]
[28 April 2022]

General provisions

Terminology and definitions

2. The definitions of terms to be used in the Convention should be made clear at the outset. In particular, there are two key terms which have been proposed to describe the subject matter of the Convention, namely “cybercrime” and “use of information and communication technologies for criminal purposes”. The term “cybercrime” is widely accepted as including cyber-dependent and cyber-enabled crime. The second term, “use of information and communication technologies for criminal purposes” would cover a wide spectrum of communication technology-related issues beyond the scope of “cybercrime”.

3. Singapore is of the view that the Convention should be based on the term "cybercrime", as it is a widely accepted term that covers the current and emerging cybercrime threats that Member States are facing. This will sharpen the focus of the Convention on the crimes which are specific to or enabled by cyberspace and will enable a more pragmatic approach to dealing with these threats.

4. There were also deliberations in the first session on whether "prevent and combat" or "counter" should be used in the Convention. Singapore prefers to use "prevent and combat", which has been used in previous instruments, including the United Nations Convention against Transnational Organized Crime.

Data privacy

5. Data privacy considerations should be balanced against the need to ensure public safety, including combating cybercrimes to ensure online safety, and allowing enforcement agencies to take necessary action to combat cybercrime quickly and effectively.

Criminalization and law enforcement

6. The Convention should also include cyberscams (which are cyber-dependent or cyber-enabled) as these make up a disproportionate percentage of all fraud in today's world. In Singapore alone, victims of scams lost at least S$633.3 million in 2021, with scam cases increasing by 52.9 per cent from the year before and making up more than half of all crimes. Scam syndicates are well-resourced and make use of technology to commit scams across national boundaries and to cover their tracks.

7. Singapore's drafting suggestions are set out below. We believe that these suggestions form a realistic and reasonable starting point on how key cyberscams can be targeted in this Convention.

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, access to the whole or any part of a computer system without right.

2. A State Party may require that the offence be committed by infringing a security measure, with the intent of obtaining computer data or other dishonest intent, such as to assume the identity of another person, or in relation to a computer system that is connected to another computer system.

Cyberfraud

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 or an entity by:

(a) Any input, alteration, deletion or suppression of computer data;

(b) Any interference with the functioning of a computer system;

(c) Using a computer system to deceive or induce another person or an entity to do or omit to do anything which the person or entity would not otherwise do or omit to do, with the fraudulent or dishonest intent of procuring for oneself or for another person, without right:

(i) An economic benefit; and/or

(ii) Computer data or personal information that would not otherwise be made available to the perpetrator.

Illegal access to passwords and credentials

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, receiving or distribution of passwords or access credentials to a computer system or computer data without right.

Procedural measures and law enforcement

Preservation, collection, obtaining and sharing of electronic evidence and data

8. On the preservation, collection, obtaining and sharing of electronic evidence and data, we would like to make three points:

(a) With more data being stored in the cloud and more transactions being carried out digitally, criminal investigations, especially in relation to cybercrime, predominantly involve digital evidence. Investigations and prosecutions will be hindered if digital evidence is not preserved, collected and obtained in a timely manner;

(b) Requests via existing channels for digital evidence, such as via mutual legal assistance treaties ("MLAT"), involve lengthy processes. If digital evidence is not preserved, collected and obtained in a timely manner, there is a high likelihood that such evidence will be overwritten by the time countries decide to accede to the MLAT request. We thus support the need for measures on lawful requests for the expedited preservation of data;

(c) Cybercrime is transnational in nature. Technological advancements have enabled criminals to carry out their activities remotely and across national borders. Provisions for cross-border sharing of electronic evidence and data will allow our law enforcement agencies to obtain actionable leads for their investigations, as well as facilitate the successful apprehension and subsequent prosecution of criminals and the recovery of assets. The Convention should allow Parties the option to reject requests if the execution of the request is likely to prejudice the sovereignty, security, public order or other essential interests of the requested Party.

9. In addition, we note that Member States have different legal systems and circumstances which could ultimately affect their ability to implement procedural measures, especially those related to the real-time collection and interception of data. We note that in most cases of cybercrime, the inclusion of measures to preserve, collect, obtain and share electronic evidence and data would already significantly benefit investigation processes, particularly in a multilateral treaty that has broad support from States. We should thus avoid being too prescriptive in terms of operational processes so that the provisions of the Convention are applicable for most States, thus allowing for wider accession/ratification. This can then allow us to tackle cybercrime more effectively in a concerted manner globally.

Asset recovery

10. Singapore has heard from many Member States on the need for an asset recovery mechanism. We support this. Cybercrime groups run sophisticated transnational operations which are not easy to detect or dismantle. They are well-resourced and adept at using technology to cover their tracks. When criminal proceeds have already been transferred out of a country, recovery is often very difficult.

11. This Convention therefore provides the opportunity to implement concrete, timely, efficient and concerted global measures to recover assets, since any country's ability to recover criminal proceeds that have already been moved out of its jurisdiction would depend on cooperation from overseas law enforcement agencies. It is important that countries work together on asset recovery so that criminal organizations do not benefit from their criminal proceeds and grow in capability, capacity and sophistication.

Uruguay

[Original: English]
[6 May 2022]

1. This Convention shall take into consideration the existing international instruments and efforts at the national, regional and international levels in preventing and combating the use of information and communications technologies for criminal purposes, in line with General Assembly resolution 74/247.

In this line, the Convention should also establish a provision on the connection between the Convention and other pre-existing instruments, including matters such as priority application and non-exclusion.

Uruguay considers that the text should include a call for coherence within the United Nations system in preventing and combating the illicit use of information and communications technologies as a general provision.

2. The Convention should be provided with a flexible mechanism for follow-up and revision, taking into consideration the progress and permanent changes existing in the matter.

The Convention should be based on neutral technological language, avoiding the use of language related to a specific operating system or software, and aiming at providing a broader approach that can be interpreted in the context of a rapidly changing environment.

Uruguay considers it important for the Convention to allow the formulation of interpretative declarations, in addition to including an agile amendment procedure to facilitate its updating and that establishes mechanisms to settle disputes.

A conference of the parties should take place periodically to study significant changes in the subject, and reflect them in the content of this Convention. Article 69, paragraph 1, of the United Nations Convention against Corruption provides a guide:

> The Conference of the States Parties shall make every effort to achieve consensus on each amendment. If all efforts at consensus have been exhausted and no agreement has been reached, the amendment shall, as a last resort, require for its adoption a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference of the States Parties.

3. The provision of instances of participation and inputs from the private sector, civil society and academia should be taken into consideration.

4. Regarding the international jurisdiction, Uruguay considers that the matter of overlapping jurisdiction of two or more States should be addresses taking into account the temporal priority in the investigation and the date of the complaint.

Nevertheless, if a State party exercising its jurisdiction under any offence established in this Convention, committed in its territory; on board a ship flying the flag of that Party; or on board an aircraft registered under the laws of that Party has been notified or has otherwise learned that any other States parties are investigating, prosecuting or conducting a judicial proceeding with respect to the same act, the competent authorities of those States parties shall, as appropriate, consult each other with a view to coordinating their actions.

The Party shall also take the measures established in this Convention when the offender is present in the territory of its country and cannot be extradited based on its nationality. The State in whose territory is located the perpetrator of the crimes established in this Convention shall submit the case without further delay to its competent authorities for the purpose of legal prosecution in accordance with the law of that State.

5. Countering cybercrime is a timely and pressing challenge that should be addressed taking into full consideration the protection, respect and fulfilment of human rights and fundamental freedoms.

All provisions of this Convention shall be understood and used in accordance with the respective international obligations in the field of human rights. Therefore, there should be a preambular paragraph reaffirming the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other relevant instruments on human rights.