Brazil's proposal on initial chapters of a United Nations convention on cybercrimes

CHAPTER I
General provisions

Article 1
Purpose

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

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

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

(c) international cooperation measures.

Commented [B1]: Source: Brazil's original proposal.

Article 2
Scope of application

1. This Convention shall apply to:
(a), ~~in accordance with its provisions, to~~ the prevention, detection, ~~suppression~~disruption, investigation, ~~and~~ prosecution and adjudication of cybercrimes~~the offences and other unlawful acts established under articles 6 to 29 of this Convention~~;
(b) ~~and to~~ the implementation of measures to ~~eliminate~~ mitigate the consequences of cybercrimes ~~such acts, including the suspension of transactions relating to assets obtained as a result of the commission of any offence or other unlawful act established under this Convention, and the seizure, confiscation and return of the proceeds of such crimes.~~; and
(c) any relevant international cooperation to prevent and counter cybercrimes.

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

Commented [Br2]: Source: China and Russia's proposal. With changes made by Brazil.

Article 3
Use of terms

For the purposes of this Convention:
(a) 'Affected person' means any person, service provider or other entity who has been, or is likely to be, affected by the grant of the any order in this Part.

(b) 'Computer data' includes any representation of data or information that has been, or is capable of being, stored, transmitted or otherwise processed in a computer system. It includes subscriber, traffic, and content data.

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

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

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

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

(g) ‘Electronic surveillance’ means:

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

ii. the monitoring or recording of activities by electronic means.

(h) ‘Service provider’ means:

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

ii. any other person, or public or private entity, that stores or otherwise processes computer data on behalf of such service or users of such service.

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

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

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

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

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

Commented [Br3]: Source: EGM UNODC MLA Model Law (process ongoing on March 9th, 2022). With minor changes made by Brazil.

CHAPTER II
Criminalization

Article 4
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 5
Data 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 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

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

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

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.

Commented [Br4]: Source: Budapest Convention.

Article 9
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 or receiving of passwords or access credentials to a computer system without right.

Commented [B5]: Source: Brazil's original proposal.

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 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 paragraphs 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 authorised 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

Commented [Br6]: Source: Budapest Convention.

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 whether or not the data is directly

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

Commented [Br7]: Source: Budapest Convention.

Article 12
Offences related to child pornography

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

(a) producing child pornography for the purpose of its distribution through a computer system;

(b) offering or making available child pornography through a computer system;

(c) distributing or transmitting child pornography through a computer system;

(d) procuring child pornography through a computer system for oneself or for another person;

(e) possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

(a) a minor engaged in sexually explicit conduct;

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

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

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.

Commented [Br8]: Source: Budapest Convention.

Article 13
Encouragement of or coercion to suicide

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.

Commented [Br9]: Source: China and Russia's proposal.

Article 14
Infringement of copyright and related rights by means of ICT

Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other 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 ICT, including the illegal use of software for copyrighted computer systems or databases and appropriation of authorship.

Commented [Br10]: Source: China and Russia's proposal.

Article 15
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 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.

Commented [Br11]: Source: Budapest Convention. With changes made by Brazil.

Article 16
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.

Commented [Br12]: Source: Budapest Convention.

Article 17
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 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.

Commented [Br13]: Source: Budapest Convention.

CHAPTER III
Procedural measures and law enforcement

Article 18
Scope of procedural provisions

1. Each ~~State party~~ Party shall adopt such legislative and other measures as are necessary to establish the powers and procedures envisaged in this ~~section~~ Chapter for the purposes of preventing, ~~identifying~~ detecting, ~~suppressing~~disrupting, ~~uncovering and~~ investigating, prosecuting and adjudicating cybercrimes ~~offences and other unlawful acts, and conducting judicial proceedings relating to such crimes~~.

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

(a) the criminal offences ~~and other unlawful acts~~ established in accordance with ~~articles 6 to 29 of this~~the Chapter II of the Convention;

(b) other criminal offences ~~and other unlawful acts~~ committed by means of ICT; and

(c) the collection of evidence in electronic form, relating to the commission of criminal offences ~~and other unlawful acts~~.

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

~~4. If a State party, owing to limitations in its domestic legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 33 and 38 of this Convention to the data being transmitted within an information system of a service provider, and that system is being operated for the benefit of a closed group of users and does not employ an information and telecommunications network and is not connected with other information systems, that State party may reserve the right not to apply those measures to such information transmission.~~

Commented [Br14]: Source: China and Russia's proposal. With changes made by Brazil.

Article 19
Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under ~~the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms,~~ the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

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

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

Commented [Br15]: Sources: Budapest Convention, as well as China and Russia's proposal.

Article 20
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 data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to 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 ninety 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. The powers and procedures referred to in this article shall be subject to Articles 18 and 19.

Commented [Br16]: Source: Budapest Convention.

Article 21
Expedited preservation of accumulated electronic information

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

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

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

4. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 18 and 19 of this Convention.

Commented [Br17]: Source: China and Russia's proposal.

Article 22
Expedited preservation and partial disclosure of traffic data

Each Party shall adopt, in respect of traffic data that is to be preserved, such legislative and other measures as may be necessary to:

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

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

The powers and procedures referred to in this article shall be subject to Articles 18 and 19.

Commented [Br18]: Sources: Budapest Convention, as well as China and Russia's proposal.

Article 23
Production order

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

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

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

2. The powers and procedures referred to in this article shall be subject to Articles 18 and 19.

~~3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:~~

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

~~(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;~~

~~(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.~~

Commented [Br19]: Sources: Budapest Convention, as well as China and Russia's proposal. With changes made by Brazil.

Article 24
Search and seizure of information stored or processed electronically

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

(a) ICT devices and information stored therein; and

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

2. Each State party shall adopt such legislative and other measures as may be necessary to ensure that where its competent authorities, conducting a search

pursuant to the provisions of paragraph 1 (a) of this article, have grounds to believe that the information sought is stored on another ICT device in the territory of that State party, such authorities shall be able to expeditiously conduct the search to obtain access to that other ICT device or the data contained therein.

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

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

(b) to make and retain copies of such information in electronic and

digital form;

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

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

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

5. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 18 and 19 of the Convention.

Commented [Br20]: Source: China and Russia's proposal. Provision similar to Art.19 of the Budapest Convention, with China and Russia's changes.

Article 25
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 co-operate 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.

4. The powers and procedures referred to in this article shall be subject to Articles 18 and 19.

Commented [Br21]: Source: Budapest Convention.

Article 26
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 co-operate 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 on specified communications 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.

4. The powers and procedures referred to in this article shall be subject to Articles 18 and 19.

Commented [Br22]: Source: Budapest Convention.

Article 27
Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

(a) in its territory; or

(b) on board a ship flying the flag of that Party; or

(c) on board an aircraft registered under the laws of that Party; or

by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over ~~the offences referred to in Article 24, paragraph 1, of this Convention, in~~ cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

~~5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.~~

Commented [Br23]: Source: Budapest Convention. With changes made by Brazil.

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

Commented [Br24]: Source: China and Russia's proposal.