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 draft provisions submitted by Member States on criminalization, general provisions and procedural measures and law enforcement

Note by the Secretariat

Summary

The present text was prepared by the Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, with the support of the secretariat. It contains the proposals received from Member States in the format of draft provisions falling under the chapters to be considered at the second session of the Ad Hoc Committee, arranged according to article, with a view to supporting Member States to identify similarities and discrepancies among the various proposals on the same topics, so as to facilitate agreement on those provisions.
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Introduction</td>
<td>5</td>
</tr>
<tr>
<td>II. Criminalization</td>
<td>5</td>
</tr>
<tr>
<td>A. General criminalization provisions</td>
<td>5</td>
</tr>
<tr>
<td>B. [Illegal] [unlawful] [unauthorized] access.</td>
<td>6</td>
</tr>
<tr>
<td>C. [Data] [digital information] interference</td>
<td>8</td>
</tr>
<tr>
<td>D. Computer [system] [network], [telecommunication network] or [electronic device] interference</td>
<td>10</td>
</tr>
<tr>
<td>E. Obstruction of a computer, programme or data</td>
<td>12</td>
</tr>
<tr>
<td>F. Disruption of information and communications technologies networks</td>
<td>12</td>
</tr>
<tr>
<td>G. Attack on a site design</td>
<td>12</td>
</tr>
<tr>
<td>H. Unauthorised access to or interference with a critical information infrastructure</td>
<td>12</td>
</tr>
<tr>
<td>I. [Illegal] [unlawful] [unauthorized] interception</td>
<td>13</td>
</tr>
<tr>
<td>J. Dishonestly receiving stolen computer resource or communication device</td>
<td>15</td>
</tr>
<tr>
<td>K. Identity-related offences</td>
<td>15</td>
</tr>
<tr>
<td>L. Unlawful use or facilitation of the unlawful use of information and communications technologies</td>
<td>16</td>
</tr>
<tr>
<td>M. Misuse of devices or creation, utilization and distribution of malicious software</td>
<td>16</td>
</tr>
<tr>
<td>N. Online Child Sexual Abuse</td>
<td>19</td>
</tr>
<tr>
<td>O. Sexual extortion</td>
<td>26</td>
</tr>
<tr>
<td>P. Non-consensual dissemination of intimate images (“revenge porn”)</td>
<td>27</td>
</tr>
<tr>
<td>Q. Offences related to pornography</td>
<td>29</td>
</tr>
<tr>
<td>R. Infringement of copyright and related rights by means of information and communications technologies</td>
<td>29</td>
</tr>
<tr>
<td>S. [Computer] [ICT]-related forgery</td>
<td>31</td>
</tr>
<tr>
<td>T. Creation and use of digital information to mislead the user</td>
<td>32</td>
</tr>
<tr>
<td>U. Violation of privacy</td>
<td>32</td>
</tr>
<tr>
<td>V. Information and communications technologies-related theft.</td>
<td>33</td>
</tr>
<tr>
<td>W. Computer- [ICT-] related fraud</td>
<td>33</td>
</tr>
<tr>
<td>X. Illicit use of electronic payment instruments</td>
<td>36</td>
</tr>
<tr>
<td>Y. Threat and blackmail</td>
<td>36</td>
</tr>
<tr>
<td>Z. Encouragement of or coercion to suicide</td>
<td>36</td>
</tr>
<tr>
<td>AA. Involvement of minors in the commission of illegal acts</td>
<td>37</td>
</tr>
<tr>
<td>BB. Incitement to subversive or armed activity</td>
<td>37</td>
</tr>
<tr>
<td>CC. Terrorism-related offences</td>
<td>38</td>
</tr>
<tr>
<td>DD. Extremism-related offences</td>
<td>39</td>
</tr>
<tr>
<td>EE. Offences related to discrimination, racism or xenophobia</td>
<td>39</td>
</tr>
<tr>
<td>FF. Sending offensive messages through communication service</td>
<td>40</td>
</tr>
<tr>
<td>GG. Offences related to the distribution of narcotic drugs and psychotropic substances</td>
<td>40</td>
</tr>
</tbody>
</table>
HH. Offences related to arms trafficking .......................................................... 40
II. Rehabilitation of nazism, justification of genocide or crimes against peace and humanity. 40
JJ. Illegal distribution of counterfeit medicines and medical products .......................... 41
KK. Use of information and communications technologies to commit acts established as offences under international law ................................................................. 41
LL. Offenses related to terrorism, arms manufacturing, trafficking in persons or drugs .......... 41
MM. Offences related to organized or transnational crime committed using information and communications technologies .......................................................... 42
NN. Computer-related criminal association ................................................................ 42
OO. Money-laundering ......................................................................................... 43
PP. Obstruction of justice .................................................................................... 45
QQ. Failure to protect data .................................................................................. 45
RR. Other illegal acts .......................................................................................... 45
SS. Liability of legal persons ................................................................................ 46
TT. Aiding, abetting, attempt .............................................................................. 49
UU. Sanctions and other measures ...................................................................... 52

III. General provisions ......................................................................................... 54
A. Statement of purpose ..................................................................................... 54
B. Scope of application ....................................................................................... 57
C. Use of terms ................................................................................................... 60
D. Protection of human rights ............................................................................ 75
E. Protection of sovereignty ................................................................................ 76
F. Effects of the Convention .............................................................................. 77

IV. Procedural measures and law enforcement ..................................................... 77
A. Jurisdiction .................................................................................................... 77
B. Scope of procedural measures ...................................................................... 84
C. Conditions and safeguards ........................................................................... 88
D. Criminal procedures ..................................................................................... 90
E. Collection of information/content and meta data transmitted by means of information and communications technologies ................................................ 91
F. Expedited preservation of stored computer data ........................................... 92
G. Expedited preservation of accumulated electronic information ..................... 93
H. Expedited preservation and partial disclosure of traffic data ........................... 94
I. Production order ................................................................................................ 98
J. Search and seizure of information stored or processed electronically or stored computer data ......................................................................................... 102
K. Real-time collection of traffic data ................................................................. 105
L. Interception of content data .......................................................................... 108
M. Retention of data .......................................................................................... 109
N. Admission of digital evidence ...................................................................... 110
<table>
<thead>
<tr>
<th></th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>O</td>
<td>Freezing, seizure and confiscation</td>
<td>110</td>
</tr>
<tr>
<td>P</td>
<td>Disposal of confiscated proceeds of crime or property</td>
<td>113</td>
</tr>
<tr>
<td>Q</td>
<td>Special investigative techniques</td>
<td>113</td>
</tr>
<tr>
<td>R</td>
<td>Establishment of criminal record</td>
<td>114</td>
</tr>
<tr>
<td>S</td>
<td>Protection of witnesses</td>
<td>114</td>
</tr>
<tr>
<td>T</td>
<td>Assistance and protection of victims</td>
<td>115</td>
</tr>
<tr>
<td>U</td>
<td>Measures to enhance cooperation with law enforcement authorities</td>
<td>115</td>
</tr>
</tbody>
</table>
I. Introduction

1. The present text was prepared by the Chair of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, with the support of the secretariat. It contains draft provisions of the convention submitted by Member States and arranged according to article, relating to the chapters of criminalization, general provision and procedural measures and law enforcement that will be discussed during the second session of the Ad Hoc Committee.

2. In preparation of the second session of the Ad Hoc Committee, the Chair prepared with support of the secretariat the parliamentary document A/AC.291/9 and its addenda, comprising a compilation of the proposals and contributions from Member States, focused on the specific chapters to be examined during the second session, as received from Member States. The differences between the current document and document A/AC.291/9 and its addenda are that in the present text proposals are arranged according to article, so that draft articles submitted by Member States on the same topic are listed together, with a view to facilitate the identification of the similarities and discrepancies among the submissions, and general comments or proposals in a format other than that of draft provisions have not been included. Where submissions by Member States shared the same content, an effort was made to group them together, with the names of Member States being ordered in alphabetical order. Information on the source of specific drafting proposals has been added by the secretariat, when mentioned in the submission or clearly identifiable. Due to the tight timeframe for preparations, the texts used were the original, non-edited, submissions in English or the unedited translations into English. Therefore, some texts may slightly differ from that contained in document A/AC.291/9 and its addenda.

3. Only proposals related to the chapters being discussed during the second session are compiled in this document. Submissions that relate to the topics of future sessions, such as prevention or international cooperation, have not been included at this time. The content of chapters was organized following most proposals received. For example, draft articles on jurisdiction were included under the chapter on procedural measures and law enforcement, and not criminalization, because most proposals had followed that approach.

4. While all efforts were made to follow a systematic and comprehensive approach, including in grouping different proposals, it is noteworthy that the original proposals, available at the website of the Ad Hoc Committee as well as in document A/AC.291/9 and its addenda, remain the reference for a complete overview of national perspectives and their context.

II. Criminalization

A. General criminalization provisions

Proposal 1

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

(Egypt)
Proposal 2

States Parties recognize as crimes for the purposes of this Convention, all criminal acts recognized by the existing International Law that are perpetrated by information technologies and electronic means.

Nothing in this Convention shall affect the rights, obligations and responsibilities of States and individuals under existing international law aimed to prevent and countering the use of ICTs for criminal purposes.

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

(Mexico)

Proposal 3

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

(Viet Nam)

Source: United Nations Convention against Transnational Organized Crime (Organized Crime Convention), article II(6), and United Nations Convention against Corruption (Convention against Corruption), article 30(9).

B. [Illegal] [unlawful] [unauthorized] access

Proposal 1

Illegal access

Each [“State”: Ghana, Jamaica, Singapore, South Africa, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: Ghana, Jamaica, United States], when committed intentionally [“and without right”: Jamaica] [“and unlawfully”: South Africa], the [“illegal”: South Africa] access to the whole or any part of a computer system without right [“without authorisation or exceeding authorised access”: Ghana] [“where committed by infringing a security measure”: European Union and its member States] [delete “without right”: Jamaica].

A [“State”: Jamaica, Singapore, United States] Party may require that the offence be committed [“where there is a breach or infringement of a security measure “: Jamaica] by infringing security measures, [deletion: European Union and its member States] with the intent of [“unlawfully”: South Africa] obtaining computer data [delete all from “by infringing security measures”: Jamaica] or other dishonest intent, [“such as to assume the identity of another person,”: Singapore] or in relation to a computer system that is connected to another computer system.

(Brazil, European Union and its member States, Ghana, Jamaica on behalf of the CARICOM, New Zealand, Singapore, South Africa, Switzerland, United Kingdom, United States)

Source: Council of Europe Convention on Cybercrime, article 2.
Proposal 2

**Illegal access**

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

(Burundi)

Proposal 3

**Illegal access to a computer system**

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

(Canada)

Proposal 4

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

**Unlawful access and/or exceeding of the limits of the right to access**

1. A person’s exceeding of the time limits or access-level limits of a right granted to that person to access a website, private account or information system.
2. Unlawful access of, presence in or contact with all or part of an information technology or the perpetuation thereof.
3. The penalty shall be increased if such access, presence, contact or perpetuation results in:
   i. The erasure, modification, distortion, copying, transfer or destruction of saved data, electronic devices or systems or communication networks, or the causing of harm to users and beneficiaries.
   ii. The obtainment of confidential government information.

(Egypt)

Proposal 5

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

**Illegal access**

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

(El Salvador)

Proposal 6

**Damage to 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 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;

(India)

Proposal 7

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.

(Malaysia)

Proposal 8

Unlawful access to digital information

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

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

C. [Data] [digital information] interference

Proposal 1

Data interference

1. Each [“State”: European Union and its member States, Malaysia, South Africa, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: European Union and its member States, United States], when committed intentionally, the [“inputting,”: Jamaica] damaging, deletion, deterioration, alteration [“, copying”: Ghana] [deletion: Malaysia] of computer data without right [without authorization: Ghana] [“or authority”: Jamaica].

2. A [“State”: European Union and its member States, Malaysia, United States] Party may reserve the right to [deletion: European Union and its member States] require that the conduct described in paragraph 1 result in serious harm [“(to natural persons, juristic persons and the economy of a State Party)” : South Africa].

(Brazil, European Union and its member States, Ghana, Jamaica on behalf of the CARICOM, Malaysia, New Zealand, South Africa, Switzerland, United Kingdom, United States)

Source: Council of Europe Convention on Cybercrime, article 4.

Proposal 2

Interference with a computer system

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

(Burundi)
Proposal 3

*Computer data interference*

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

(Canada)

Proposal 4

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

*Attack on data integrity*

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

(Egypt)

Proposal 5

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

*Data interference*

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

(El Salvador)

Proposal 6

*Damage to 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 permission of the owner or any other person who is in charge of a computer, computer system or computer network,

(b) downloads, copies or extracts any data, computer data base 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 data base or any other programmes residing in such computer, computer system or computer network;

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

(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) steal, conceal, 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.
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 programme, 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.

(India)

Proposal 7

Unlawful interference with digital information

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

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

Proposal 8

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

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

To steal, modify, sabotage or counterfeit information or data;

(Viet Nam)

D. Computer [system] [network], [telecommunication network] or [electronic device] interference

Proposal 1

Each [“State”: European Union and its member States, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: European Union and its member States, United States], when committed intentionally [“and unlawfully”: South Africa], the serious hindering without right [without authorisation: Ghana] of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

(Brazil, European Union and its member States, Ghana, New Zealand, South Africa, Switzerland, United Kingdom, United States)

Source: Council of Europe Convention on Cybercrime, article 5.

Proposal 2

Data interference

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

(Burundi)
Proposal 3

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

(Canada)

Proposal 4

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

Interference with computer system

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

(El Salvador)

Proposal 5

Damage to 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 permission of the owner or any other person who is in charge of a computer, computer system or computer network,

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base 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;

(India)

Proposal 6

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.

(Jamaica on behalf of the CARICOM)

Proposal 7

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

To obstruct or disturb normal operations of a computer network, telecommunications network or an electronic device;
To take control or interfere in the operation of an electronic device by bypassing security or protection system, abusing the rights of administration of another person, or any other means;

(Viet Nam)

E. **Obstruction of a computer, programme or data**

Proposal 1

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.

(Malaysia)

F. **Disruption of information and communications technologies networks**

Proposal 1

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

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

G. **Attack on a site design**

Proposal 1

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

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

(Egypt)

H. **Unauthorised access to or interference with a critical information infrastructure**

Proposal 1

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

*Unauthorized access to critical information infrastructure*

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

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

(Egypt)

Proposal 2

Unauthorised access to a critical information infrastructure

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

(Ghana)

Proposal 3

Unlawful interference with critical information infrastructure

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

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

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

I. [Illegal] [unlawful] [unauthorized] interception

Proposal 1

Illegal interception

Each [“State”: European Union and its member States, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: European Union and its member States, United States], when committed intentionally [“and unlawfully”: South Africa], the interception without right [without authorisation: Ghana], made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

A [“State”: European Union and its member States, United States] 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.

(Brazil, European Union and its member States, Ghana, New Zealand, South Africa, Switzerland, United Kingdom, United States)

Source: Council of Europe Convention on Cybercrime, article 3.
Proposal 2

**Illegal interception of non-public computer system transmission**

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

(Canada)

Proposal 3

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

**Unlawful interception**

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

(Egypt)

Proposal 4

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

**Unlawful interception**

When committed intentionally and without right, the interception without due authorization, carried out by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

(El Salvador)

Proposal 5

**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 a dishonest intent, or in relation to a computer system that is connected to another computer system.

(Jamaica on behalf of the CARICOM)

Proposal 6

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.

(Malaysia)
Proposal 7

Unlawful interception

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

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

J. Dishonestly receiving stolen computer resource or communication device

Proposal 1

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.

(India)

K. Identity-related offences

Proposal 1

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 [“or distribution”: Singapore] of passwords or access credentials to a computer system [“or computer data”] without right.

(Brazil, Singapore)

Proposal 2

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.

(India)

Proposal 3

Unauthorized access to personal data

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

(Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan)
L. Unlawful use or facilitation of the unlawful use of information and communications technologies

Proposal 1

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

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

(Egypt)

M. Misuse of devices or creation, utilization and distribution of malicious software

Proposal 1

Misuse of devices

1. Each [“State”: European Union and its member States, Jamaica, South Africa, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: European Union and its member States, Jamaica] [Sentence starts with “Establish as criminal offences”: Canada], when committed intentionally [“and unlawfully”: South Africa] and without right:

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

   (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the [“cybercrime”: Canada] [“criminal”: Jamaica] offences established in accordance with [“Articles 4 through 9”: Brazil] [Articles (Unauthorized/Illegal Access, Unauthorized/Illegal Interception / Data Interference/ System Interference)”: Jamaica] [“with the preceding articles of this chapter”: United States] [“with the provisions on illegal access, illegal interception, data interference or system interference of this Convention”: Switzerland] [“included in this convention”: Canada];

   (ii) a computer password, access code, or similar data by which the whole or any part of a computer system [“an information, communication and technology system”: Jamaica] is capable of being accessed,

   with intent that it be used for the purpose of committing any of the [“cybercrime”: Canada] [“criminal”: Jamaica] offences established in [“Articles 4 through 9”: Brazil] [“Articles (Unauthorized/ Illegal Access, Unauthorized/ Illegal Interception/ Data Interference/ System Interference)”: Jamaica] [“established in the preceding articles of this chapter”: United States] [“established in accordance with the provisions on illegal access, illegal interception, data interference or system interference of this Convention”: Switzerland] [“included in this convention”: Canada]; and

   (b) the possession of an item referred to in paragraphs a.i or ii above [deletion: Canada], with intent that it be used for the purpose of committing any of the [“cybercrime”: Canada] [“criminal”: Jamaica] offences established in [“Articles 4 through 9”: Brazil] [Articles (Unauthorized/ Illegal Access, Unauthorized/ Illegal Interception/ Data Interference/ System Interference).”: Jamaica] [“established in the preceding articles of this chapter”: United States] [“established in accordance with the provisions on illegal access, illegal interception, data interference or system interference of this Convention”: Switzerland] [“included in this convention”: Canada]. A [“State”: European Union and its member States, Jamaica] Party may require by law [deletion of “by law”: European Union and its member States, Switzerland] that a number of such items be possessed before criminal liability attaches. [deletion: Canada]
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 [deletion: Canada] is not for the purpose of committing an [“a criminal”: Jamaica] offence [“a cybercrime offence”: Canada] established in accordance with [“Articles 4 through 9 of this Convention”: Brazil] [“Articles (Unauthorized/ Illegal Access, Unauthorized/ Illegal Interception/ Data Interference/ System Interference) of this Convention”: Jamaica] [“with the preceding articles of this chapter”: United States] [“with the provisions on illegal access, illegal interception, data interference or system interference of this Convention”: Switzerland] [“included in this Convention”: Canada], such as for the authorised testing or protection of a computer system.

(Brazil, Canada, European Union and its member States, Ghana, Jamaica on behalf of the CARICOM, New Zealand, South Africa, Switzerland, United Kingdom, United States)

3. Each [“State”: European Union and its member States, Jamaica, South Africa, United States] Party may reserve the right [deletion: European Union and its member States] not to [deletion: European Union and its member States] apply paragraph 1 of this article, provided that the reservation [“it”: European Union and its member States] does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article.

(Brazil, European Union and its member States, Ghana, Jamaica on behalf of the CARICOM, New Zealand, South Africa, Switzerland, United Kingdom, United States)

Source: Council of Europe Convention on Cybercrime, article 6.

Proposal 2

Creation, utilization and distribution of malicious software

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

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

Illegal trafficking in devices

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

The provisions of this article shall apply when the manufacture, sale, purchase for use, import, export or other form of transfer for use of devices is related, for example, to an authorized trial or to protection of a computer system.

(Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan)
Proposal 3

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

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

(Burundi)

Proposal 4

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

Misuse of devices

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

(El Salvador)

Proposal 5

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

Misuse of information technology

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

(Egypt)

Proposal 6

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.

(Malaysia)

Proposal 7

Each Member State shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed unauthorizedly and intentionally:
(a) To manufacture, trade, transfer instruments, equipment or software meant to attack a computer network, telecommunications network or an electronic device which to be used for criminal activities as governed in this Convention;

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

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

(Viet Nam)

N. Online Child Sexual Abuse

Proposal 1

Article [A] – child abuse material through a computer system

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

   (a) accessing, controlling, transmitting, distributing, offering, procuring, producing, or making available child abuse material through a computer system², or

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

2. For the purposes of Article [A], the term ‘child abuse material’ shall include material that depicts or describes a child, or a representation of a child, who is implied to be, or appears to be engaging in sexual activities or in the presence of a person engaging in sexual activities, any representation of the sexual parts of a child³ for primarily sexual purposes, or a victim of torture, cruel, inhumane, or degrading treatment or punishment.

Article [B] – facilitation of child abuse material through a computer system

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally [without lawful excuse]⁴ creating, developing, altering, maintaining, controlling, moderating, assisting⁵, making available, advertising or promoting a computer system for the purposes of facilitating child abuse material as identified in Article [A].

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

¹ This caveat is included to ensure the offence does not unintentionally capture certain legitimate situations – for example, where there may be a medical requirement to access or produce material which would otherwise be captured by this provision.

² ‘Computer system’ defined to mean any device or group of interconnected or related devices, where one or more of them performs automatic processing of data pursuant to a program. This may include input, output and storage facilities. It would also include standalone systems or one networked with other devices. Note that this term (or its definition) may be altered to ensure consistency with other provisions of the draft convention.

Self-generated material may cover both material which is purely self-generated, and also coerced or extorted self-generated material. In these contexts, the provision aims to provide a general stance of extra caution around criminalisation but still leaving it to domestic legal systems to decide on their own proportionate and reasonable response.


⁴ As per footnote 2.

⁵ ‘Assisting’ may ultimately be captured by extensions of criminal responsibility general provisions. Retained here until those provisions are considered.
Article [C] – grooming or procuring of a child for sexual purposes through a computer system

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, through a [computer system] grooming, making a proposal, procuring or causing a child, to meet, witness, or participate in sexual activities.

Article [X] – general provisions related to the proposal

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

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

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

(Australia)

Proposal 2

Offences related to child pornography/child sexual exploitation and abuse/content-related offences

1. Each [“State”: Jamaica, Russian Federation, South Africa] Party shall [“also”: Russian Federation] adopt such legislative and other measures as may be [“are”: Russian Federation] necessary to establish as criminal offences [an offence: Russian Federation] under its domestic law [delete: Jamaica] [“the following acts, committed intentionally and unlawfully”: Russian Federation] [start sentence with “Establish as criminal offences”: Canada], when committed intentionally and without right [“and unlawfully”: South Africa], the following conduct:

   (a) producing child pornography/child sexual exploitation [“and abuse”: Jamaica, Switzerland, United Kingdom] [material: Canada, Jamaica, Switzerland, United Kingdom] [“child sexual abuse materials”: South Africa] for the purpose of its distribution through a computer system [“through an information and communications technology system”: Jamaica] [“or information and communication technologies”: South Africa] [“through information and communication networks, including the Internet”: Russian Federation];

   (b) offering, [“advertising.”: Canada] or making available child pornography/child sexual exploitation [“and abuse”: Jamaica, Switzerland, United Kingdom] [“material”: Canada, Jamaica, Switzerland, United Kingdom] [“child sexual abuse materials”: South Africa] through a computer system [“or information and communications technologies”: South Africa] [“through an information and communications technology system”: Jamaica] [“through information and communication networks, including the Internet”: Russian Federation];

6 The addition of belief here is intended to cover situations where a person of interest or person being investigated for grooming or procuring children for sexual purposes, is engaging with a law enforcement officer online in an undercover capacity.
(c) distributing or transmitting child pornography/child sexual exploitation [“and abuse”: Jamaica, Switzerland, United Kingdom] [“material”: Canada, Jamaica, Switzerland, United Kingdom] [“child sexual abuse materials”: South Africa] through a computer system [“through an information and communications technology system”: Jamaica] [“or information and communications technologies”: South Africa] [“using information and communication networks, including the Internet, to distribute, transmit, publicly display, or advertise child pornography”: Russian Federation];

(d) procuring child pornography/child sexual exploitation [“and abuse”: Jamaica, Switzerland, United Kingdom] [“material”: Canada, Jamaica, Switzerland, United Kingdom] [“child sexual abuse materials”: South Africa] through a computer system [“/ information and communications technology system for oneself or for another person”: Jamaica] [“or information and communications technologies”: South Africa] for oneself or for another person [“using ICT to procure child pornography oneself or for another person”: Russian Federation];

(e) [“accessing or”: Canada] possessing child pornography/child sexual exploitation [“and abuse”: Jamaica, Switzerland, United Kingdom] [“material”: Canada, Jamaica, Switzerland, United Kingdom] [“child sexual abuse materials”: South Africa] in a computer system [“/ information and communications technology system or on a computer-data storage medium”: Jamaica] [“or information and communications technologies”: South Africa] or on a computer-data storage medium [“or on electronic digital data storage devices”: Russian Federation].

[“(f) viewing child sexual exploitation and abuse material in a computer system or on a computer-data storage”: United Kingdom]

(Brazil, Canada, Jamaica on behalf of the CARICOM, Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan, South Africa, United Kingdom)

2. For the purpose of paragraph 1 above [“of this article”: Russian Federation], the term “child pornography” [“child sexual exploitation and abuse material”: Jamaica, Switzerland, United Kingdom] [“child sexual abuse materials”: South Africa] shall include pornographic [deletion: Jamaica, Switzerland, United Kingdom] material that visually depicts:

(a) a [deletion: South Africa] minor [“child”: Jamaica] engaged in [“real or simulated”: United Kingdom] sexually explicit conduct;

(b) a person appearing to be a minor [“child”: Jamaica] engaged in [“real or simulated”: United Kingdom] sexually explicit conduct; [“and”: South Africa]

(c) realistic images representing a minor engaged in [“real or simulated”: United Kingdom] sexually explicit conduct.

[“(d) any depiction of a minor’s sexual organs for primarily sexual purposes”: United Kingdom]

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

(Brazil, Jamaica on behalf of CARICOM, Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan, South Africa, Switzerland, United Kingdom)

Source: Council of Europe Convention on Cybercrime, article 9, in part.

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.

(Brazil, South Africa, Switzerland, United Kingdom)
3. For the purpose 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.

(Jamaica on behalf of CARICOM)

Source: Convention on the Rights of the Child, article 1

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.

(Brazil, Switzerland, United Kingdom)

Alternative paragraph 2:

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

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

(i) a child engaged in or in the presence of sexual activity,
(ii) a person appearing to be a child engaged in or in the presence of sexual activity,
(iii) realistic images representing a child engaged in or in the presence of sexual activity;

(b) written material that:

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

(c) audio recordings that:

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

(Canada)

Proposal 3

Offences relating to child pornography

The States Parties to this Convention shall establish as criminal offences, without prejudice to their domestic law, the following conduct, when committed intentionally and without right: producing child pornography for the purpose of its distribution through a computer system; offering or making available child pornography through a system.

(Burundi)

Proposal 4

Grooming and luring of a child

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

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

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

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

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

(Canada)

Proposal 5

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

Offences related to material with child abuse content

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

(El Salvador)

Proposal 6

Offences related to child sexual exploitation and abuse online

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

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

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

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

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

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

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

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

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

3. For the purpose of this section, child sexual exploitation and abuse material includes a material image, visual recording, video, audio, live streaming material, drawing or text, that depicts or describes
(a) A child engaged in sexually explicit or suggestive conduct;

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

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

(d) Sexually explicit images of children;

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

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

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

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

Dealing with a child for purposes of sexual abuse

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally the use of

(a) a computer online service,

(b) an internet service,

(c) a local bulletin board service, or

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

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

Cyberstalking of a child

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally the use of a computer online service, an internet service, or a local internet bulletin board service or any other electronic device to compile, transmit, publish, reproduce, buy, sell, receive, exchange, or disseminate the name, telephone number, electronic mail address, residence address, picture, physical description, characteristics or any other identifying information on a child in furtherance of an effort to arrange a meeting with the child for the purpose of engaging in sexual intercourse, sexually explicit conduct, or unlawful sexual activity.

(Ghana)

Proposal 7

Publishing or transmitting of material depicting children in 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.

(India)

Proposal 8

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

   (a) making, producing, 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; or

   (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 has in the person 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 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

(Malaysia)

Proposal 9

“computer-related offenses involving child sexual abuse materials”

1. Each State Party shall take the necessary legislative or other measures to ensure that the following conduct, when committed knowingly and through a computer system, is criminalized:
(a) Producing child sexual abuse material;
(b) Causing the live transmission of a child engaged in sexually explicit conduct;
(c) Offering or making available child sexual abuse material;
(d) Distributing or transmitting child sexual abuse material;
(e) Procuring child sexual abuse material for oneself or for another person;
(f) Possessing child sexual abuse material;
(g) Knowingly obtaining access, through information and communication technologies, to child sexual abuse material or viewing the live transmission of a child engaged in sexually explicit conduct.

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

(United States)

O. Sexual extortion

Proposal 1

Sexual extortion

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

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

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

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

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

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

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

(Ghana)
P. **Non-consensual dissemination of intimate images (“revenge porn”)**

**Proposal 1**

*Non consensual dissemination of intimate images (“Revenge porn”)*

1. Establish as criminal offences, when committed intentionally and without right, publishing, distributing, transmitting, selling, making available, or advertising an intimate image of a person by any means of a computer system, knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct.

2. For the purpose of paragraph 1, intimate image means a visual recording of a person made by any means including a photographic, film, or video recording:
   - *(a)* in which the person is nude, is exposing their genital organs, anal region or breasts, or is engaged in explicit sexual activity;
   - *(b)* in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
   - *(c)* in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.

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

(Canada)

**Proposal 2**

*Non-consensual sharing of intimate image*

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

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

**Threat to distribute prohibited intimate image or visual recording**

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

(Ghana)

**Proposal 3**

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:
“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 the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means 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 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.

Proposal 4

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 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.

Proposal 5

Posting or distributing an intimate visual recording without consent

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

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

(b) being reckless as to whether the victim has consented to the posting.
For clarity, a child or young person under the age of 16 years cannot consent to the posting of an intimate visual recording of which they are the subject.

(New Zealand)

Q. Offences related to pornography

Proposal 1

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

Pornography

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

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

Other Crimes Related to Pornography

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

(Egypt)

Proposal 2

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 the 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.

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.

(India)

R. Infringement of copyright and related rights by means of information and communications technologies

Proposal 1

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 [illegal: Russian Federation] 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.
Proposal 2

**Offences related to infringements of intellectual property and related rights**

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

(Burundi)

Proposal 3

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

**Offences related to infringement of copyright or related rights**

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

(Egypt)

Proposal 4

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

**Infringement of intellectual property and related rights**

The infringement of intellectual property and related rights as defined in the legislation of the State Party when such acts are premeditated and committed through the use of ICTs, including the unlawful use of computer programs and databases, which are protected by copyright, and plagiarism.

(El Salvador)

Proposal 5

**Offences related to infringements of copyright and related rights**

1. Each [“State”: South Africa, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: United States] the infringement of copyright, as defined under the law of that [“State”: United States] Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty [under the various international treaties and agreements: South Africa], with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system ["or information and communications technologies": South Africa].

2. Each [“State”: South Africa] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights

---

7 Consistent with BC and AUC.
and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system [“or information and communications technologies”: South Africa].

3. A [“State”: South Africa, United States] Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

(Ghana, South Africa, United Kingdom, United States)

Source: Council of Europe Convention on Cybercrime, article 10.

Proposal 6

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.

(Jamaica on behalf of the CARICOM)

S. [Computer] [ICT]-related forgery

Proposal 1

Computer-related forgery

Each [“State”: Jamaica, South Africa, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: Jamaica, United States], 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 [“State”: Jamaica, United States] Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

(Brazil, Ghana, Jamaica on behalf of the CARICOM, New Zealand, South Africa, Switzerland, United States)

Source: Council of Europe Convention on Cybercrime, article 7.

Proposal 2

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

Falsification

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

(Egypt)

Proposal 3

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

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

(El Salvador)

T. Creation and use of digital information to mislead the user

Proposal 1

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

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

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

U. Violation of privacy

Proposal 1

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

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

(Egypt)

Proposal 2

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.

(India)

Proposal 3

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

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

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

(Viet Nam)
V. Information and communications technologies-related theft

Proposal 1

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

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

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

W. Computer- [ICT-]related fraud

Proposal 1

Each [“State”: Jamaica, South Africa, United States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: Jamaica, United States], when committed intentionally [“and unlawfully”: South Africa] 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, [delete: Jamaica] an economic benefit for oneself or for another person.

(Brazil, Ghana, Jamaica on behalf of the CARICOM, New Zealand, South Africa, Switzerland, United States)

Source: Council of Europe Convention on Cybercrime, article 8.

Proposal 2

Computer-related fraud

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

(1) Fraud in computer systems

The States Parties to this Convention shall establish as a criminal offence, without prejudice to their domestic law, the use of a fraudulent scheme, by means of electronic communication, to obtain or attempt to obtain money, movable property, bonds, deposits, instruments, pledges, receipts, releases, or the whole or any part of the property of another person.

(2) Digital identity theft

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

(3) **Phishing**

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

(4) **Breach of trust in relation to computer data**

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

(5) **Unlawful receiving of computer data**

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

(6) **Extortion of computer data**

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

(7) **Blackmail and publishing of rumors**

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

(8) **Spamming**

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

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

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

(Burundi)

**Proposal 3**

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

**Fraud**

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

(Egypt)
Proposal 4

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

*Fraud by means of ICTs*

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

(El Salvador)

Proposal 5

*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 personation.

(India)

Proposal 6

*Cyber fraud*

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right, the causing of a loss of property to another person 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 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.

(Singapore)

Proposal 7

*Fraud*

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

(a) fraud by false representation,

(b) fraud by failing to disclose information,

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

(United Kingdom)
Proposal 8

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

To use a computer network, telecommunications network or electronic device for the following purposes:

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

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

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

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

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

(Viet Nam)

X. Illicit use of electronic payment instruments

Proposal 1

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

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

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

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

4. The knowing acceptance of a forged payment instrument.

(Egypt)

Y. Threat and blackmail

Proposal 1

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

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

(Egypt)

Z. Encouragement or coercion to suicide

Proposal 1

Encouragement of or coercion to suicide
Each [“State”: Russian Federation] Party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the encouragement of or coercion to suicide, including of minors, through psychological or other pressure over [“in”: Brazil] information and telecommunication networks, including the Internet.

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

**Proposal 2**

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

The encouragement or coercion, including of minors, to commit suicide, through psychological or other pressure over information and communication networks, including the Internet, whether through direct interaction or through modern technologies and electronic games.

(Egypt)

### AA. Involvement of minors in the commission of illegal acts

**Proposal 1**

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

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

(Egypt)

**Proposal 2**

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

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

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

### BB. Incitement to subversive or armed activity

**Proposal 1**

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

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

(Egypt)

**Proposal 2**

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

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

CC. Terrorism-related offences

Proposal 1

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

1. Dissemination, advocacy or justification of the ideas and principles of terrorist groups.
2. Financing of or training for terrorist acts, facilitation of communication between terrorist organizations or the provision of logistical support for perpetrators of terrorist acts.
3. Dissemination of methods for making explosives employed in particular in terrorist acts.
4. Spreading of strife, sedition, hatred or racism.
5. States shall take the necessary measures to prevent the dissemination of such content via ICTs, including blocking or removing content related to these offences.

(Egypt)

Proposal 2

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 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 cause the denial of access to any person authorised to access computer resource; or

      (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised 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 authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base 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 cyber terrorism.

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 para 1 (a) and 1(b).

(India)
Proposal 3

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

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

Proposal 4

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

To use cyberspace, information technologies or electronic devices to undertake an act of terrorism or terrorist financing.

(Viet Nam)

DD. Extremism-related offences

Proposal 1

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

The distribution of materials that call for illegal acts with political, ideological, social or ethnic motives or any other illegal act advocating ethnic or religious hatred or enmity in general, by means of ICTs, or the advocacy, justification or provision of access to such acts.

(Egypt)

Proposal 2

1. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law the distribution of materials that call for illegal acts motivated by political, ideological, social, racial, ethnic, or religious hatred or enmity, advocacy and justification of such actions, or to provide access to such materials, by means of ICT.
2. Each State party shall adopt such legislative and other measures as are necessary to establish as an offence or other illegal act under its domestic law humiliation by means of ICT of a person or group of people on account of their race, ethnicity, language, origin or religious affiliation.

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

EE. Offences related to discrimination, racism or xenophobia

Proposal 1

Racist or xenophobic text and images through a computer system

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

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

(Burundi)

FF. Sending offensive messages through communication service

Proposal 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 sends, by means of a computer resource or a communication device,

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

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such 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.

(India)

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

Proposal 1

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

(Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan, South Africa)

HH. Offences related to arms trafficking

Proposal 1

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

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

II. Rehabilitation of nazism, justification of genocide or crimes against peace and humanity

Proposal 1
Each State party shall adopt such legislative and other measures as are necessary to establish as an offence under its domestic law the intentional dissemination by means of ICT of materials that deny, approve or justify actions that amount to genocide or crimes against peace and humanity, established by the Judgment of the International Military Tribunal formed under the London Agreement of 8 August 1945.

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

**JJ. Illegal distribution of counterfeit medicines and medical products**

**Proposal 1**

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

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

**KK. Use of information and communications technologies to commit acts established as offences under international law**

**Proposal 1**

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

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

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

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

**LL. Offenses related to terrorism, arms manufacturing, trafficking in persons or drugs**

**Proposal 1**

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

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

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

---

8 The Annex referred to in this proposal can be found in the submission by Russian Federation, contained in document A/75/980.
(1) Establishing, publishing or using the website of a terrorist group with the aid of the Internet, a computer or a computer system in order to facilitate communication by its leadership or members;

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

(2) Dissemination of methods or means of destruction

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

(3) Creation or publication of a site for the purpose of trafficking in human beings

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

(4) Creation or publication of a site for the purpose of trafficking in or distributing drugs or narcotics

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

(Burundi)

MM. Offences related to organized or transnational crime committed using information and communications technologies

Proposal 1

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

1. Promotion of or trafficking in narcotic drugs or psychotropic substances.
2. Illicit distribution of counterfeit medicines or medical products.
3. Smuggling of migrants.
4. Illicit trafficking of persons or human organs.
5. Illicit arms trade.
6. Illicit trafficking in cultural property.

(Egypt)

NN. Computer-related criminal association

Proposal 1

Computer-related criminal association

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

(Burundi)
**OO. Money-laundering**

**Proposal 1**

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

*Financial offences, including money-laundering*

1. Use of ICTs to commit financial offences, or the misuse of virtual currencies (digital and encrypted).
2. Conduct of money-laundering operations, requesting of assistance to conduct money-laundering operations, or the publication of money-laundering methods.

(Egypt)

**Proposal 2**

*Laundering of proceeds of crime committed through the use of ICTs*

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

- The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;
- The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;
- The acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime;
- Participation in, association or conspiracy to commit, attempts to commit and aiding, instigating, facilitating and counselling the commission of any of the offences established in accordance with this Convention.

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

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

(b) Include as predicate offences the offences established in accordance with the articles of this Convention. In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in such list a comprehensive range of offences associated with organized criminal groups;

(c) For the purposes of subparagraph (b), predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;

(d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations.

(El Salvador)
Proposal 3

Criminalisation of money laundering

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

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

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

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

   (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of cybercrime [crime: United States];

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

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

   (a) Each State Party shall seek to apply paragraph 1 of this article to the widest range of predicate offences; [deletion: United States]

   (b) Each State Party shall include as predicate offences relevant crimes established in relevant article of this Convention and [deletion: United States] the offences established in accordance with [relevant articles: New Zealand] [the criminalization articles: United States] of this Convention. In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in such list [a comprehensive range of offences associated with cybercrime: New Zealand] [include the offences that are set forth in this convention: United States];

   (c) For the purposes of subparagraph (b), predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;

   (d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;

   (e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence;

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

   (New Zealand, United States)

Source: Organized Crime Convention, article 6, and Convention against Corruption, article 23.
**PP. Obstruction of justice**

Proposal 1

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

(a) The use of physical force, threats or intimidation or the promise, offering or giving of an undue advantage to induce false testimony or to interfere in the giving of testimony or the production of evidence in a proceeding in relation to the commission of offences covered by this Convention;

(b) The use of physical force, threats or intimidation to interfere with the exercise of official duties by a justice or law enforcement official in relation to the commission of offences covered by this Convention. Nothing in this subparagraph shall prejudice the rights of States Parties to have legislation that protects other categories of public officials.

(El Salvador, New Zealand, United States)

*Source: Organized Crime Convention, article 11, and Convention against Corruption, article 30.*

**QQ. Failure to protect data**

Proposal 1

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.

(India)

**RR. Other illegal acts**

Proposal 1

This Convention shall not prevent a State party from criminalizing any other unlawful act committed intentionally through ICTs.

(Egypt)

Proposal 2

*Other Unlawful acts committed using ICTs*

Without prejudice to (Article on protection of Sovereignty) the Contracting Parties shall mutually agree on any other unlawful acts committed using ICTs for the purpose of cooperation established under this Convention. (There should be a provision in this Convention titled “Other Unlawful Acts” considering the advancement in ICT technologies). In addition, the following cybercrimes may be further extended as criminalization through the UNODC document 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

(India)

Proposal 3

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

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

Proposal 4

Nothing in this Convention shall prevent Member States to adopt such legislative and other measures as may be necessary to establish as criminal offences of any other act involving the use of ICTs for criminal purposes.

(Viet Nam)

SS. Liability of legal persons

Proposal 1

Corporate liability/Liability of legal persons

1. Each [“State”: Jamaica, Russian Federation] Party shall adopt such legislative and other [delete: Jamaica] [“legal”: Russian Federation] measures as may be [are: Russian Federation] necessary [“, consistent with its legal principles”: Jamaica] to ensure that legal persons can be held liable for a criminal offence [“or other illegal act”: Russian Federation] established in accordance with this Convention [“established as such under this Convention”: Russian Federation], [“when such an offence or act was”: Russian Federation] committed for their benefit by any natural person, acting either individually or as part of an organ [“entity”: Russian Federation] of the [“respective”: Russian Federation] legal person, who has a leading position within it, based on [“and holding a leadership position within it by virtue of”: Russian Federation] [“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”: Jamaica]:

(a) A power of representation [attorney: Russian Federation] of the legal person;

(b) An [deletion: Russian Federation] authority to take decisions on behalf of the legal person;

(c) An [deletion: Russian Federation] authority to exercise [“supervision or”: Jamaica] control within the legal person.

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

3. Subject to the legal principles [“domestic law”: Jamaica] of the [“State”: Jamaica, Russian Federation] Party, the liability of a legal person may be criminal, civil or administrative. [“The State party shall ensure that legal persons held liable are subject to effective, proportionate and dissuasive sanctions, including monetary sanctions”: Russian Federation].

4. Such liability [“of legal persons”: Russian Federation] shall be without prejudice to the criminal [deletion: Russian Federation] liability of the natural persons who have committed the [“criminal”: Jamaica] offence [“or other illegal act”: Russian Federation].

(Brazil, Ghana, Jamaica on behalf of the CARICOM, Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan, Switzerland)

Source: Council of Europe Convention on Cybercrime, article 12.

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.

(Jamaica on behalf of the CARICOM)

Proposal 2

Chapter III. Liability of legal persons

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

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

(Burundi)

Proposal 3

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

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

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

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

(Canada)

Sources: Organized Crime Convention, article 10, and Convention against Corruption, article 26.

Proposal 4

Liability of legal entities

1. Each State party shall undertake, subject to its domestic law, to regulate the criminal liability of legal persons for offences committed by their representatives in

9 This proposal was submitted by Canada under the chapter of “General provisions”.

V.22-03252 47/116
their name or for their benefit, without prejudice to the punishment of natural persons—
including site administrators—who commit offences.

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

   (a) The saving and storage of the following data in an information system log
     or information technology log for a period of (to be determined):
     – Data that enable the identification of service users.
     – Data related to the content that is processed on information systems when such
data are under the control of the service provider.
     – Data related to communication traffic.
     – Data related to communication peripherals.
     – Any other data specified by the State for the purposes of implementing this
       Convention.

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

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

   (d) Provision of easy, direct and continuous access to the following data and
     information for users of its services and any competent authority:
     – The name and address of the service provider.
     – The contact information of the service provider, including its email address.
     – Licensing data that identifies the service provider and the competent authority
       that supervises it.

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

(Egypt)

Proposal 5

Liability

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

In addition to the cases provided for in the preceding paragraph, each State Party
shall take the measures necessary to ensure that a legal person can be held liable where
the lack of supervision or control by a natural person referred to in the preceding
paragraph has made possible the commission of an offence established in accordance
with this Convention for the benefit of that legal person by a natural person acting
under its authority.
Subject to the legal principles of the State Party, such liability may be criminal, civil or administrative. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

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

(El Salvador)

Proposal 6
Liability of legal persons
1. Each State Party shall adopt such legislative and other measures as may be necessary, consistent with its legal principles, to ensure that legal persons can be held liable for a criminal offence established in accordance with Articles 5 to 10 of this Convention.
2. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

(European Union and its member States)

Proposal 7
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 Article 5 to 10 of this Convention.
2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.
3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.
4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

(Malaysia, New Zealand, United States)

Source: Organized Crime Convention, article 10, and Convention against Corruption, article 26.

5. Legal persons shall be protected from liability for an act done or omitted to be done in good faith—
   (a) in the performance or intended performance of a duty imposed by or under this convention; or
   (b) in the exercise or intended exercise of a function or power conferred by or under this convention.

(New Zealand)

TT. Aiding, abetting, attempt

Proposal 1
Attempt and aiding or abetting
1. Each [“State”: European Union and its member States] Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: European Union and its member States], when committed intentionally, aiding or abetting the commission of any of the offences established in accordance [with the Chapter II] [“Articles 5 through 19”: Ghana] [“with the provisions on criminalization of this Convention”: Switzerland] of the [“present”: Ghana] [“this”: European Union and its member States, Switzerland, United Kingdom] Convention [“with intent that such offence be committed”: Ghana, Switzerland, United Kingdom].

2. Each [“State”: European Union and its member States] Party shall [“may”: European Union and its member States] adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law [deletion: European Union and its member States], when committed intentionally, an attempt to commit any of the offences established in accordance with the Chapter II [with the provisions on criminalization: Switzerland] of the [this: European Union and its member States, Switzerland, United Kingdom] Convention [Articles 7 through 9, 11, 12, 13 (1) (a) (b) and (e), 14, 15, 16, 17: Ghana].

   (Brazil, Ghana, European Union and its member States, Switzerland, United Kingdom)

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

   (Brazil, Switzerland, United Kingdom)

Source: Council of Europe Convention on Cybercrime, article 11, with modifications.

Proposal 2

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

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

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

   (Canada)

Source: Convention against Corruption, article 27.

Proposal 3

Attempted commission or participation in the commission of an offence

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

   (Egypt)

Proposal 4

States should adopt appropriate legislative and other measures to establish as criminal offences under their national law – imposing criminal and other sanctions,

---

10 This proposal was submitted by Canada under the chapter of “General provisions”. 
including imprisonment, that take into account the number of victims and the extent of the damage caused – the following acts:

**Aiding or abetting and attempt**

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

(El Salvador)

**Proposal 5**

*Damage to 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 permission of the owner or any other person who is in charge of a computer, computer system or computer network,

(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, rules or regulations made thereunder;

**Proposal 6**

*Participation and attempt*

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, [delete: Jamaica] [“abetting or”: Malaysia] participation in any capacity such as an accomplice, assistant or instigator [“, abettor or conspirator”: Jamaica] 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, [delete: Jamaica] 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, [delete: Jamaica] the preparation for an offence established in accordance with this Convention.

(Jamaica on behalf of the CARICOM, Malaysia, New Zealand, United States)

**Proposal 7**

*Aiding, preparing and attempting the commission of an offence*

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

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

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

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

UU. Sanctions and other measures

Proposal 1

Sanctions and measures

1. Each [“State”: Jamaica] Party shall [“adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with [relevant chapter or provision] of the Convention are punishable by”: Brazil, Ghana, Switzerland] [“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”: Jamaica] effective, proportionate and dissuasive sanctions, which include [: including the”: Jamaica] deprivation of liberty.

2. Each [“State”: Jamaica] Party shall ensure that legal persons held liable in accordance with [relevant provision] shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

(Brazil, Ghana, Jamaica on behalf of CARICOM, Switzerland)

Source: Council of Europe Convention on Cybercrime, article 13.

Proposal 2

Prosecution, adjudication and sanctions

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

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

In the case of offences established in accordance with the articles of this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.

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

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

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

(El Salvador)
Source: Organized Crime Convention, article 11, and Convention against Corruption, article 30.

Proposal 3
Prosecution, adjudication and sanctions

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

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

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

(European Union and its member States)

Proposal 4
Prosecution, adjudication and sanctions

1. Each [“State”: Malaysia, United States] Party shall make the commission of an offence established in accordance with [“the criminalization articles of”: United States] this Convention liable to sanctions that take into account the gravity of that offence.

2. Each [“State”: Malaysia, United States] Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by this Convention are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.

3. In the case of offences established in accordance with [“the criminalization articles of”: United States] this Convention, each [“State”: Malaysia, United States] 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”: Malaysia, United States] 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.

(Malaysia, United Kingdom, United States)

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

(United Kingdom, United States)

6. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of [“the”: United States] conduct is reserved to the domestic law of a [“State”: Malaysia, United States].
States] Party and that such offences shall be prosecuted and punished in accordance with that law.

(Malaysia, United Kingdom, United States)

Source: Organized Crime Convention, article 11.

Proposal 5

Establishment of liability

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

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

III. General provisions

A. Statement of purpose

Proposal 1

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.

(Brazil)

Proposal 2

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

(Canada)

Proposal 3

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

(a) To promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively,
(b) To promote and facilitate international cooperation,
(c) To ensure a high level of protection of victims’ rights and
(d) To support capacity building and technical assistance in the fight against cybercrime.

(European Union and its member States)

Proposal 4

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

(Egypt)

Proposal 5

The purpose of this convention is to promote and facilitate international cooperation as well as strengthen measures to prevent and counter the use of ICTs for criminal purposes.

(Ghana)

Proposal 6

The purposes of this Convention are as follows:

1. To promote and strengthen measures aimed at preventing and combatting 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.

(Jamaica on behalf of the CARICOM)

Proposal 7

1. To promote and strengthen measures to prevent and combat cybercrime;
2. To promote, facilitate, and strengthen international cooperation; and
3. To provide practical tools to enhance technical assistance and build the capacity of national authorities.

(Japan)

Source: Chair’s proposal [A/AC.291/CRP8].

Proposal 8

The purposes of this Convention are:

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

(b) To promote and facilitate international cooperation;

(c) To 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.

(Malaysia)
Proposal 9

The purpose of this Convention is to promote bilateral and multilateral cooperation and legal assistance, including multi-sectorial cooperation, to prevent, respond, investigate, mitigate and prosecute the use of ICTs for criminal purposes.

(Mexico)

Proposal 10

The aims of this Convention are:

To promote the adoption and strengthening of measures to effectively prevent and combat ICT-related crimes and other illegal acts;

To prevent actions targeting the confidentiality, integrity and availability of ICT, and to prevent the misuse of ICT, by making punishable the acts covered by this Convention, and by providing powers sufficient to effectively combat such crimes and other illegal acts, by facilitating their detection, investigation and prosecution at both the domestic and international level and by developing arrangements for international cooperation;

To improve the efficiency of international cooperation, and to develop such cooperation, including in the area of training and the provision of technical assistance for preventing and combating ICT-related crimes.

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

Proposal 11

The objectives of the Convention shall be:

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

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

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

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

(South Africa)

Proposal 12

The purposes of this Convention are:

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

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

(Switzerland)
Proposal 13

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

(United Kingdom of Great Britain and Northern Ireland)

Proposal 14

Objectives:

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

(b) To promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against the use of ICTs for criminal purposes, including asset recovery, in accordance with fundamental principles of international law and in a manner of respecting human rights.

(Viet Nam)

B. Scope of application

Proposal 1

1. This Convention shall apply to:

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

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

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

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

(Brazil)

Source: Proposal by China and the Russian Federation, with modifications.

Proposal 2

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

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

2. To promote, facilitate and support international cooperation and assistance in relation to the prevention, investigation and prosecution of offences established in this convention;

3. To promote, facilitate and support efficient and effective mutual legal assistance in relation to electronic evidence pertaining to the offences established in this convention and any other criminal offences; and

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

(Canada)

Proposal 3

This Convention shall apply, except as otherwise stated herein, to:
(a) The prevention, investigation and prosecution of criminal offences established in accordance with articles 5 to 10 of this Convention, and

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

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

(European Union and its member States)

Proposal 4

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

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

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

(Egypt)

Proposal 5

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

1. The Prevention, investigation and prosecution of offences established in accordance with Articles 5 through 20 and

2. 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

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

(Ghana)

Proposal 6

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.

(Jamaica on behalf of the CARICOM)

Proposal 7

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.

(Malaysia)

Proposal 8

This Convention shall apply, in accordance with its provisions, to the prevention, detection, suppression, investigation and prosecution of the offences and other illegal acts recognized as such under articles 6–29 of this Convention and to the implementation of measures to eliminate the consequences of such acts, including the suspension of transactions relating to assets obtained as a result of the commission of any crime or other illegal act established as such under this Convention, and the seizure, confiscation and return of the proceeds of such crimes.

For the purposes of implementing this Convention, it shall not be necessary for the crimes and other illegal acts referred to in it to result in material damage, except as otherwise provided herein.

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

Proposal 9

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

(South Africa)

Proposal 10

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

(Switzerland)

Proposal 11

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.

(United Kingdom of Great Britain and Northern Ireland)

Proposal 12

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

(United States of America)

Proposal 13

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

(Viet Nam)
C. **Use of terms**

**Proposal 1**

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.

(Brazil)

Source: UNODC expert group meeting on mutual legal assistance model law, with modifications.

Proposal 2

For the purposes of this Convention:

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

“Encryption” means any technique that transforms digital data into an unintelligible format by using cryptological means.

“Cryptology” means the science of protecting and securing information.

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

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

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

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

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

“Computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

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

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

“Information” means any element of knowledge that can be represented with the aid of devices in order to be used, preserved, processed or communicated. Information may be expressed in written, visual, audio, digital or other forms.
“Critical infrastructure” means infrastructure that is essential to services vital for public safety, economic stability, national security and international stability and for the sustainability and restoration of critical cyberspace.

The critical infrastructure facilities of the State consist of services relating to public health, internal and external security, defence, finance and transport that are connected to Internet networks.

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

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

“Means of electronic payment” refers to means by which the holder is able to make electronic payment transactions online.

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

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

1. The production of such visual depiction involves a minor;
2. Such visual depiction is a digital image, computer image or computer-generated image in which a minor is engaging in sexually explicit conduct, or where images of the sexual parts of a minor are produced or used for primarily sexual purposes and exploited with or without the child’s knowledge;
3. Such visual depiction has been created, adapted or modified to give the impression of a minor engaging in sexually explicit conduct.

“Service providers” means mobile operators, Internet service providers and infrastructure operators.

“Computer program” means a set of instructions executed by the computer to achieve the intended result.

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

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

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

“ICT” means information and communications technology.

(Burundi)

Proposal 3

“Computer system” means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or telecommunications functions.
“Computer data” means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

“Traffic data” means any computer data to identify, activate or configure a device relating the creation, transmission or reception of a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination or termination, route, time, date, size, duration, or type of underlying service.

“Service provider” means:

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, including over the Internet; and

(b) any other entity that processes or stores computer data that is available over the Internet.

Source: Council of Europe Convention on Cybercrime, article 1, with modifications.

Proposal 4

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

(2) Computer data: “... any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function”.

(3) Service provider: “... any public or private entity that provides to users of its services the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service”.

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

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

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

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

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

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

(10) Subscriber information: “... any information ... that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: ... the type of communication service used, the technical provisions taken thereto and the period of service ... the subscriber’s identity, postal
Proposal 5

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

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

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

3. Data: all such information as may be stored, processed, generated and transmitted by information technology, such as numbers, letters, symbols and the like.

4. Information system: a set of programmes and tools designed to process and manage data and information.

5. Information network: two or more information systems that are linked to obtain and exchange information.

6. Site: a place where information is made available on an information network through a specific address.

7. Capture: the viewing or obtainment of data or information.

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

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

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

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

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

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

14. Digital evidence: any electronic evidentiary information that is stored on or transmitted, extracted or obtained from computers, information networks and the like and that can be collected and analysed using special technological devices, software or applications.
15. Traffic (traffic data): data that are produced by an information system and that show a communication’s origin, destination, sender, addressee, route, time, date, size and duration and the type of service.

(Egypt)

Proposal 6

Terminology

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

“Computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform an action.

“Service provider” means any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.

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

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

(El Salvador)

Proposal 7

For the purpose of this Convention:

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

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

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

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

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

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

(h) “Service provider” shall mean:

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

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

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

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

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

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

(j) “Traffic data” shall mean any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, data, size, duration, or type of underlying service;

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

(European Union and its member States)

Source: Council of Europe Convention on Cybercrime, article 1, in part.

Proposal 8

For the purpose of this Convention

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

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

(c) “Content data” means the communication content of the communication, that is, the meaning or purport of the communication or the message or information being conveyed by the communication other than traffic data;

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

(e) “Critical information Infrastructure” means a computer or computer system identified by a member state in its domestic legislation as essential for national security or the economic and social well-being of citizens.

(f) “Prohibited intimate image and visual recording” includes
(i) Moving or still image that depicts
   a. The person engaged in an intimate sexual activity that is not ordinarily done in public; or
   b. The genital or anal region of a person, when the genital or anal region is bare or covered only by underwear; and
(ii) An image that has been altered to appear to show any of the things mentioned in paragraph (I) even if the thing has been digitally obscured, if the person is depicted in a sexual way;

(g) Service Provider means:

   (i) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
   (ii) Any other entity that processes or stores computer data on behalf of such communication service or users of such service;

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

(i) “Subscriber Information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of the services of a service provider other than traffic or content data and by which may be established;

   (i) The type of communication service used, the technical provision taken in respect of the communication service and the period of service;
   
   (ii) The identity, postal or geographic address, telephone and other access number of the subscriber, billing and payment information available on the basis of the service agreement or arrangement; and
   
   (iii) Any other information on the site of the installation of a communication equipment, available on the basis of the service agreement or arrangement

(j) “Traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the origin, destination, route, time, date, size or duration of the communication or the type of underlying service;

(Ghana)

Source: Council of Europe Convention on Cybercrime, article 1, with modifications.

Proposal 9

Terms of usage

(i) “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;

(ii) “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;

(iii) “computer network” means the inter-connection of one or more computers or computer systems or communication device through–

   (a) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
(b) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained;

(iv) “computer resource” means computer, computer system, computer network, data, computer data base or software;

(v) “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;

(vi) “computer contaminant” means any set of computer instructions that are designed—

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

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

(vii) “computer data-base” 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 formalised 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;

(viii) “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;

(ix) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

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

(xi) “cyber security” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction;

(xii) “data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised 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;

(xiii) “information” includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer-generated micro fiche;

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

(xv) “reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorised 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 State parties in consultation with such professional bodies or associations as it may deem fit;

(xvi) “sensitive personal data or information” means such personal information as may be prescribed by the State parties in consultation with such professional bodies or associations as it may deem fit.

(xvii) “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.

(xviii) Social Media Intermediary: 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.

(xix) Electronic Record: It means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

(xx) Originator: It 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.

(xxii) “Property”: It 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.

(xxiii) “Proceeds of Crime”: It shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence or other unlawful act as established under this convention.

(xxiv) “Confiscation”: It includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority.

(xxv) “Predicate Offence: It 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.

(xxvi) “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.

(India)

Proposal 10

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, authorise 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 offenses 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;

Proposal 11

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

“computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer to perform such a function.

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

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

Proposal 12

For the purposes of this Convention:

(a) “Seizure of property” shall mean the temporary prohibition of the transfer, conversion, disposition or movement of property, or the temporary assumption of custody or control of property pursuant to an order of a court or other competent authority;

(b) “Botnet” shall mean two or more ICT devices on which malicious software has been installed and which are controlled centrally without the knowledge of users;

(c) “Malicious software” shall mean software the purpose of which is the unauthorized modification, destruction, copying, and blocking of information, or neutralization of software used to secure digital information;

(d) “Child pornography” shall have the meaning given to that term under article 2 (c) of the Optional Protocol of 25 May 2000 to the Convention on the Rights of the Child, on the sale of children, child prostitution and child pornography;

(e) “Proceeds” shall mean any property derived from or obtained, directly or indirectly, through the commission of any crime or other illegal act covered by this Convention, as well as income or other benefit derived from such proceeds, from property into which such proceeds have been transformed or converted or from property with which such proceeds have been intermingled;
(f) “Information and communications technologies” (ICT) shall mean processes and methods of generating, processing and distributing information, as well as ways and means of their implementation;

(g) “Information and telecommunications networks” shall mean a set of engineering equipment designed to control technological processes by means of computer technology and telecommunications;

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

(i) “Information” shall mean any data (messages, records), irrespective of the form in which it is presented;

(j) “Confiscation” shall mean the forcible deprivation of property without compensation pursuant to an order of a court or other competent authority;

(k) “Computer attack” shall mean the targeted interference of software and/or hardware and software with information systems or information and telecommunications networks to disrupt and/or terminate their functioning and/or threaten the security of information processed by such facilities;

(l) “Digital information” shall mean any data (records), irrespective of form and characteristics, contained and processed in information and telecommunications devices, systems and networks;

(m) “Critical information infrastructure” shall mean an assemblage of critical information infrastructure facilities and telecommunications networks used to interconnect critical information infrastructure facilities;

(n) “Critical infrastructure facilities” shall mean information systems and information and communications networks of public authorities and information systems and automated process control systems operating in the defence, health-care, education, transport, communications, energy, banking and finance sectors, nuclear and other important areas of the life of the State and society;

(o) “Service provider” shall mean:

(i) Any public or private entity that provides to users of its services the ability to communicate by means of ICT, or

(ii) Any other entity that processes or stores electronic information on behalf of an entity referred to in (i) above or the users of the services provided by such entity;

(p) “Traffic data” shall mean any electronic information (excluding the contents of the transferred data) relating to the transfer of data by means of ICT and indicating, in particular, the origin, destination, route, time, date, size, duration and type of the underlying network service;

(q) “ICT device” shall mean an assemblage (grouping) of hardware components used/designed for automatic processing, storage and transfer of electronic information;

(r) “Electronic evidence” shall mean any evidentiary information stored or transmitted in digital form (on an electronic medium).

The term “substantial harm” shall be determined in accordance with the domestic law of the requested State Party.

(Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan)
Proposal 13

For the purposes of this Convention:

“article” means any—

(a) data;

(b) computer program;

(c) computer data storage medium; or

(d) computer system,

which—

(i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;

(ii) may afford evidence of the commission or suspected commission; or

(iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission, of—

(aa) an offence in terms of this Convention;

(bb) any other offence brought about through the use of information and communications technologies; or

(cc) an offence in a foreign State that is substantially similar to an offence contemplated in this Convention;

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

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

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

(c) such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct.

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

“computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

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

“computer program” means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

“computer system” means—

(a) one computer; or
(b) two or more inter-connected or related computers, which allow these inter-connected or related computers to—

(i) exchange data or any other function with each other; or

(ii) exchange data or any other function with another computer or a computer system;

“confiscation”, which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

“cyber dependant crimes” are offences that can only be committed using a computer, computer networks or other form of information communications technology;

“cyber enabled crimes” are crimes which do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology.

“data message” means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form;

“digital information” means any data (records), irrespective of form and characteristics, contained and processed in information and communication devices, systems and networks;

“electronic evidence” shall mean any evidentiary information stored or transmitted in digital form (on an electronic medium);

“freezing of assets” shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

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

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

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

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

“service provider” means any public or private entity that provides to users of its service the ability to communicate by means of a computer system, or any other entity that processes or stores computer data on behalf of such communication service or users of such service.

“traffic data” means data relating to a communication indicating the communication’s origin, destination, route, format, time, date, size, duration or type, of the underlying service.

(South Africa)

Source: Organized Crime Convention, article 2, in part, as applicable.

Proposal 14

“Computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.
“Computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

“Service provider” means:

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

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

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

(Switzerland, United Kingdom of Great Britain and Northern Ireland)

Source: Council of Europe Convention on Cybercrime, article 1.

Proposal 15

“child” means any individual under the age of 18.

“child sexual abuse material” shall mean any visual depiction or live transmission of (1) a child engaged in real or simulated sexually explicit conduct or (2) an adult engaged in real or simulated sexuality explicit conduct with a child intentionally included in the visual depiction or live transmission. It shall not be necessary for the child to be conscious or aware of, or able to appraise the nature of, such sexually explicit conduct.

“computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform such a function.

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

“confiscation”, which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority.

“cybercrimes” mean offenses established in accordance with this Convention.

“freezing” or “seizure” shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority.

“predicate offence” shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in the criminalization of the laundering of proceeds of cybercrime article of this Convention.

“proceeds of crime” shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence.

“property” shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.

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

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

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

“sexually explicit conduct” includes at least the following real or simulated acts:

(a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse in a sexual context; or (e) lascivious exhibition of the genitals or the pubic area of a child, whether clothed or nude.

“traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

(United States of America)

Source: Council of Europe Convention on Cybercrime, article 1, or Organized Crime Convention, article 2, or the Convention on the Rights of the Child, article 1, as applicable, with modifications.

Proposal 16

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

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

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

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

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

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

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

(Viet Nam)

D. Protection of human rights

Proposal 1

Decided to take actions of prevention, response, mitigation, investigation and prosecution to effectively protect people and in particular vulnerable groups from the use of information and communication technologies for criminal purposes.

(Mexico)
Proposal 2

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

(United Kingdom of Great Britain and Norther Ireland)

Proposal 3

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

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

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

(United States of America)

E. Protection of sovereignty

Proposal 1

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

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

(Egypt)

Proposal 2

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

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

(Ghana, Jamaica on behalf of the CARICOM, Malaysia, South Africa, United States, Viet Nam)

Source: Convention against Corruption, article 4, and Organized Crime Convention, article 4.

Proposal 3

1. The States parties shall carry out their obligations under this Convention in accordance with the principles of State sovereignty, the sovereign equality of States and non-interference in the internal affairs of other States.
2. This Convention shall not authorize the competent authorities of a State party to exercise in the territory of another State party the jurisdiction and functions that are reserved exclusively for the authorities of that other State under its domestic law, except as otherwise provided for in this Convention.

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

F. Effects of the Convention

Proposal 1

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

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

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

(European Union and its member States)

Source: Council of Europe Convention on Cybercrime, article 39, with modifications.

IV. Procedural measures and law enforcement

A. Jurisdiction

Proposal 1

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[“5 through 20”: Ghana] 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
   (d) 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. [“For the purpose of the extradition article of this Convention,”: Ghana] 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”: Colombia] [“the offences established in accordance with this Convention, in”: Ghana] 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. [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: Brazil] [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: Colombia and Ghana].

(Brazil, Colombia and Ghana)

Source: Council of Europe Convention on Cybercrime, article 22 (with modifications by Brazil).

Proposal 2

1. Each State Party shall adopt the necessary measures to establish its jurisdiction over the offences established in this convention when:

   (a) the offence is committed in the territory of that State Party;
   
   (b) the offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the domestic law of that State Party at the time that the offence is committed; or
   
   (c) the offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory.

2. Enable a State Party 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.

3. Enable a State Party to establish its jurisdiction over the offences established in accordance with this convention when the alleged offender is present in its territory and it does not extradite him or her.

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

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

(Canada)

Proposal 3

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

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

---

11 This proposal was submitted by El Salvador under the chapter on criminalization.
A State Party may also establish its jurisdiction over any such offence when:

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

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

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

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

If a State Party exercising its jurisdiction in accordance with the preceding paragraphs has been notified, or has otherwise learned, that another State Party is conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

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

(El Salvador)

Source: Convention against Corruption, article 42, and Transnational Organized Crime Convention, article 15, with modifications.

Proposal 4

1. Each State Party shall adopt such measures as may be necessary to establish jurisdiction over the offence established in accordance with Articles 5 to 10 of this Convention when:

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

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

(c) The offence is committed 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. State Party may also establish its jurisdiction over any such offence when:

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

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

3. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and it does not extradite him or her, solely on the basis of his or her nationality, after a request for extradition.

4. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that one or more 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.

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

(European Union and its member States)
Proposal 5

Data oriented jurisdiction

Data oriented jurisdiction means that the country whose citizen’s data is being stored/processed/screened/federated anywhere in the world should be having the broader jurisdiction of the data immaterial of where the data is 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.

“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 resource 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 State 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 ICTs.

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.

(India)
Proposal 6

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 State 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.

(Malaysia, United Kingdom)

Source: Convention against Corruption, article 42, and Transnational Organized Crime Convention, article 15, which modification.

Proposal 7

1. Each State party shall take all measures necessary to establish jurisdiction over criminal offences and other illegal acts established as such under this Convention, when they are committed:
   (a) In the territory of that State party; or
   (b) On board a vessel flying the flag of that State party when the offence was committed, or on board an aircraft registered under the law of that State party at that time.

2. Subject to article 3 of this Convention, a State party may also establish its jurisdiction over any such offence and other illegal act when:
   (a) The offence is committed against a national of that State party, a stateless person permanently residing in its territory, a legal person established or having a permanent representation in its territory, a State or government facility, including the premises of a diplomatic mission or consular office of that State party; or
   (b) The offence is committed by a national of that State party or a stateless person whose habitual residence is in its territory; or
   (c) The offence is committed against that State party; or
(d) The offence is committed wholly or partly outside the territory of that State party but its effects in the territory of that State party constitute an offence or result in the commission of an offence.

3. For the purposes of article 47 of this Convention, each State party shall take all measures necessary to establish its jurisdiction over the offences established as such under this Convention when the alleged offender is present in its territory and the State party does not extradite such person solely on the grounds that he or she is a national of that State party or a person to which it has granted refugee status.

4. Each State party in whose territory an alleged perpetrator is present and which does not extradite such person shall, in cases provided for in paragraphs 1 and 2 of this article, without any exception and regardless of whether the offence was committed in the territory of that State party, 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. 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.

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

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

Proposal 8

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

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

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

2. Subject to article 4 [“the sovereignty article”: United States] of this Convention, a State Party may also establish its jurisdiction over any such offence [“involving the use of information and communications technologies”: South Africa] when:

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

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

   (c) The offence is one of those established in accordance with article 17, paragraph 1 (b) (ii) [“with Article [money laundering article]”: United States] of this Convention and is committed outside its territory with a view to the commission of an offence [“involving the use of information and communications technologies”: South Africa] established in accordance with article 15 [Article [money laundering article]: United States] of this Convention within its territory; or

   (d) The offence is committed against the State Party [“, or has direct impact on the affairs of such State Party”: South Africa].

3. For the purposes of article … [on Extradition] of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over

---

12 This proposal was submitted by South Africa under the chapter on criminalization.
the offences [“involving the use of information and communications technologies”: South Africa] established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over [“the”: South Africa] offences [“involving the use of information and communications technologies”: South Africa] 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.

(South Africa, United States)

Source: Convention against Corruption, article 42, and Organized Crime Convention, article 15, which modification.

Proposal 9

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

   (a) in its territory; or

   (b) 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; or

   (c) by one of its nationals, if the offence is punishable under the law of the State in which 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 established in accordance with the provisions on criminalization 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, provided that the offences are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

4. A Party may also establish its jurisdiction over any offence established in accordance with the provisions on criminalization of this Convention, when the offence is committed:

   (a) against a national of that Party

   (b) against that Party.

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

6. 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.

(Switzerland)

Proposal 10\(^1\)

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

\((a)\) The offence is committed in the territory of that State Party
\((b)\) The offence is committed on board a vessel that is flying a flag of that State Party or an aircraft that is registered under the laws of that State Party
\((c)\) The offence is directed against computer system, device or data or person located in the territory of that State Party
\((d)\) The offence is committed by or against a national of that State Party.

(United Republic of Tanzania)

Proposal 11

1. Each Member State shall take such measures as may be necessary to establish its jurisdiction over the offences referred to in articles … in the following cases:

\((a)\) When the offences are committed in any territory under its jurisdiction or on board a ship or aircraft registered in that State;
\((b)\) When the alleged offender is a national of that State;
\((c)\) When the victim is a national of that State if that State considers it appropriate.

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

(Viet Nam)

B. Scope of procedural measures

Proposal 1

1. Each Party shall adopt such legislative \(\text{"and other" Brazil}\) measures as are necessary to establish \(\text{"the": Brazil}\) powers and procedures \(\text{"envisaged in this Chapter": Brazil}\) for the purposes of preventing, \(\text{"identifying.": Egypt}\) detecting, \(\text{"disrupting.": Brazil}\) investigating \(\text{"", prosecuting and adjudicating": Brazil}\) cybercrimes, \(\text{"for the purposes of preventing, identifying, detecting and investigating offences and other illegal acts and conducting judicial proceedings relating thereto": Egypt}\).

2. \(\text{"Except as otherwise provided,"}: Brazil\) Each \(\text{"State": Egypt}\) Party shall apply the \(\text{"aforementioned": Egypt}\) powers and procedures \(\text{"referred to in paragraph 1 of this article": Brazil}\) to:

\(\text{(a) the criminal offences established in accordance with the Chapter II of the Convention \"The criminal offences and other illegal acts set forth in this Convention": Egypt};\)

\(\text{(b) other criminal offences \"and other illegal acts": Egypt}\) committed by means of ICT; and

\(^{13}\) This proposal was submitted by Tanzania under the chapter on general provisions.
(c) the collection of evidence in electronic form, relating to the commission of criminal offences [“The collection of electronic evidence”: Egypt].

(Brazil, Egypt)

Sources: China and Russia's proposal, with modifications.

Proposal 2

1. Clarify that powers and procedures provided for in this section are for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise, a State Party shall apply the powers and procedures referred to in paragraph 1 to:
   
   (a) the criminal offences established in accordance with this convention;
   
   (b) other criminal offences committed by means of a computer system; and
   
   (c) the collection of evidence in electronic form of a criminal offence.

(Canada)

Proposal 3

1. Each [“State”: Jamaica] Party shall adopt such [delete: Jamaica] legislative and other measures as may be necessary to establish the powers and procedures provided for in this section [“Chapter”: Jamaica] for the purpose of specific [delete: Jamaica] criminal investigations or proceedings.

2. [“Except as specifically provided otherwise in Article 21,”: Colombia] [“Except as otherwise provided in Article (Interception of Communication)”: Jamaica] Each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
   
   (a) the criminal offences established in accordance with [Articles 2 through 11: Colombia] [the provisions on criminalization: Jamaica, Switzerland] of this Convention;
   
   (b) other criminal offences committed by means of a computer system [“of an information, communication and technology system”: Jamaica]; and
   
   (c) the collection of evidence in electronic form of a criminal offence.

3. (a) Each Party may reserve the right to apply the measures [referred to in Article 20: Colombia] [on real-time collection of traffic data: Jamaica, Switzerland] only to [“criminal”: Jamaica] offences or categories of offences [delete: Jamaica] specified in the reservation, provided that the range of such offences or categories of offences [delete: Jamaica] is not more restricted than the range of [“criminal”: Jamaica] offences to which it [“the State Party”: Jamaica] applies the measures referred to in [Article 21: Colombia] [on interception of content data: Jamaica, Switzerland]. Each Party shall consider restricting such a reservation to enable the broadest application of [the measure referred to in Article 20: Colombia] [measures referred to in Article 20: Colombia] [measures on real-time collection of traffic data: Switzerland] [delete: Jamaica].

   (b) Where a [“State”: Jamaica] Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply [the measures referred to in Articles 20 and 21: Colombia] [measures referred on real-time collection of traffic data and on interception of content data: Jamaica, Switzerland] 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”: Jamaica] Party may reserve the right not to apply these measures to such communications. Each [“State”: Jamaica] Party shall consider restricting such a reservation to enable the broadest application of [the measures referred to in Articles 20 and 21: Colombia] [measures on real-time collection of traffic data and on interception of content data: Jamaica, Switzerland].

(Colombia, Jamaica on behalf of the CARICOM, Switzerland)

Source: Council of Europe Convention on Cybercrime, article 14.

Proposal 4

1. Each [State: United States] Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise [in the article addressing interception of content data: United States], each [State: El Salvador, United States] Party shall apply the powers and procedures referred to in [“the preceding”: El Salvador] paragraph 1 [delete: El Salvador] of this article to:

   (a) the criminal [delete: El Salvador] 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.

(El Salvador, Malaysia, United Kingdom, United States)

Proposal 5

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

2. 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 5 through 10 of this Convention; and

   (b) The collection of evidence in electronic form of a criminal offence established in accordance with Articles 5 through 10 of this Convention.

(European Union and its member States)

Proposal 6

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

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

   (a) the criminal offences established in accordance with Articles 5 through 20 of 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.

3. Each Party may reserve the right to apply the measures referred to in Article 29 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in [in the article on
interception of content data]. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 29.

4. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 29 and 30 to communications being transmitted within a computer system of a service provider, which system:

    (a) is being operated for the benefit of a closed group of users, and

    (b) Does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 29 and 30.

5. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Article 31 that Party may reserve the right not to apply these measures. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Article 31.

(Ghana)

Proposal 7

1. Each State party shall adopt such legislative and other measures as are necessary to establish the powers and procedures envisaged in this section for the purposes of preventing, detecting, suppressing, exposing and prosecuting offences and other illegal acts, and conducting judicial proceedings relating to such offences and acts.

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

   (a) The criminal offences and other illegal acts established in accordance with articles 6–29 of this Convention;

   (b) Other criminal offences and other illegal acts committed by means of ICT;

   (c) The collection of evidence, including electronic evidence, relating to the commission of criminal offences and other illegal acts.

3. (a) 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;

   (b) 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 information being transmitted within an information system of a service provider, and that system

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

      (ii) 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.

(Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan)
Proposal 8

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 article for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 32, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

   (a) the criminal offences involving the use of information and communications technologies established in accordance with Articles --- through --- of this Convention;

   (b) other criminal offences committed by means of information and communications technologies; and

   (c) the collection of evidence in electronic form of a criminal offence involving the use of information and communications technologies.

3. Each State Party may reserve the right to apply the measures referred to in Article 31 only to offences or categories of offences involving the use of information and communications technologies specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to Article 32. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Article 31.

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 Articles 31 and 32 to communications being transmitted using information and communications technologies of a service provider, which system:

   (a) is being operated for the benefit of a closed group of users, and

   (b) does not employ public communications networks and is not connected with other information and communications technologies, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 31 and 32.

(South Africa)

C. Conditions and safeguards

Proposal 1

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section [“Article”: Jamaica] are subject to conditions and safeguards provided for under its domestic law, which shall provide for [“ensure”: Russian Federation] the adequate [delete: Jamaica] [“and full”: European Union and its member States] protection of human rights and liberties [“freedoms”: Russian Federation] [“fundamental freedoms”: European Union and its member States], including rights arising pursuant to [“from the”: Russian Federation] obligations it [“that the State Party”: Russian Federation] has undertaken under [“the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.”: Colombia] [“the International Bill of Human Rights including the 1948 Universal Declaration on Human Rights,” :Ghana] [“the 1948 Universal Declaration of Human Rights,”: European Union and its member States] the 1966 United Nations International Covenant on Civil and Political Rights, [“the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, the 1989 Convention on the Rights of the Child, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography”: European Union and its member States] and other applicable
international [“and regional”: Switzerland] human rights instruments [“law”: United Kingdom], and which shall incorporate the principle of proportionality [delete: Jamaica, Russian Federation] [“and necessity and ensuring judicial oversight”: Ghana] [“and which shall incorporate the principles of proportionality, legality and necessity and the protection of privacy and personal data”: European Union and its member States].

2. Such conditions and safeguards shall, as appropriate [delete: Russian Federation] in view of the nature of the procedure or power [“powers and procedures”: Russian Federation] concerned [“such conditions and safeguards shall include,”: Russian Federation], inter alia, include [delete “, include”: Russian Federation] judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure [“powers or procedures”: Russian Federation].

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each [“the”: Russian Federation] [“State”: Jamaica] Party shall consider the impact of the [“these”: Jamaica] powers and procedures [“provided for”: Russian Federation] in this section [“Article”: Jamaica] upon the rights, responsibilities and legitimate interests of third parties.

(Brazil, Colombia, European Union and its Member States, Ghana, Jamaica on behalf of the CARICOM, Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan, United Kingdom)

Source: Council of Europe Convention on Cybercrime, article 15, with modifications.

Proposal 2

1. Each State Party shall ensure that the establishment, implementation and application of the provisions of this convention are subject to conditions and safeguards provided for under its domestic law, which shall provide for the full protection of human rights and liberties, including rights arising pursuant to obligations under the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principles of the rule of law, legality, necessity and proportionality.

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

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

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

(Canada)

14 This proposal was submitted by Canada under the chapter on general provisions.
Proposal 3

Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this section are subject to the conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and freedoms.

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

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 the powers and procedures provided for in this section on the rights, responsibilities and legitimate interests of third parties.

(El Salvador)

Proposal 4

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 adequate protection of human rights and liberties, including rights and fundamental freedoms arising pursuant to obligations it has undertaken under agreements, treaties, applicable international human rights instruments, and which shall incorporate the principle of proportionality consistent with the sovereignty of the State Party.

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

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

(South Africa)

D. Criminal procedures

Proposal 1

Criminal procedures shall include:

1. The expeditious preservation of data stored in ICTs, including user tracking information that has been stored on information technology, particularly if it is believed that such information is subject to loss or modification, by issuing an order obliging the person concerned to preserve the integrity of such data in his/her possession or control to enable the competent authorities to search and investigate, while maintaining the confidentiality of any actions taken in this regard.

2. The expeditious preservation and partial disclosure of user tracking information regardless of how many service providers were involved in the transmission of such information, and assurance of the expeditious disclosure by the competent authorities of a fair amount of traffic data to enable the State party to identify the service providers and the transmission path of the communication.

3. Orders to provide information in the possession of a person in the territory of a State party and stored on an information technology or storage medium, or in the
possession or control of a service provider that provides services in the territory of the State party.

4. Inspection of stored information or access to information stored on an information technology or storage medium.

5. Seizure, copying and retention of stored information in order to conduct procedures for searching and accessing it.

6. Real-time collection of user tracking information and the obliging of service providers within the jurisdiction of the State party to collect, record and maintain the confidentiality of such information.

7. Interception of content information by enabling the competent authorities to collect and record, in real time through technical means, the information transmitted by ICTs.

8. Each State party shall take the necessary legislative and other measures to enable its competent authorities to stop the transmission and broadcast of any content that constitutes an offence set forth in this Convention.

(Egypt)

E. Expedited preservation of stored computer data

Proposal 1

1. Each [“State”: European Union and its member States] 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 [“information and communications technologies”: South Africa], in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a [“State”: European Union and its member States, South Africa] 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 [“180 days”: India] [“seven days”: South Africa], to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each [“State”: European Union and its member States, South Africa] 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.

(Brazil, Colombia, European Unions and its member States, Ghana, India, South Africa, Switzerland, United Kingdom)

4. The powers and procedures referred to in this article shall be subject to Articles [18 and 19] [14 and 15] [19 and 20] [27 and 28] [the articles on scope of procedural measures, and on conditions and safeguards: Switzerland] [“human rights safeguards”: United Kingdom].

(Brazil, Colombia, European Unions and its member States, Ghana, South Africa, Switzerland, United Kingdom)

Source: Council of Europe Convention on Cybercrime, article 17.
Proposal 2

1. Each State Party shall adopt such legislative and other measures [“as may be necessary”: El Salvador, United States] 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 [“If”: Canada] a State 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 State Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A State Party may provide for such an order to be subsequently renewed.

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

(Canada, El Salvador, United States)

Source: Council of Europe Convention on Cybercrime, article 17.

Proposal 3

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 is 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 & Safeguards).

(Jamaica on behalf of the CARICOM)

F. Expedited preservation of accumulated electronic information

Proposal 1

1. Each State party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to give adequate orders or instructions or similarly 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 State 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 is 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 State party shall also 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] [31 and 32] of this Convention.

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

G. Expedited preservation and partial disclosure of traffic data

Proposal 1

Each [“State”: Jamaica] Party shall adopt, in respect of traffic data that is to be preserved under the provisions of article 34 of this Convention [delete “under the provisions of article 34 of this Convention: Brazil”] [“the article on expedited preservation of stored computer data”: Colombia] [“the article on corporate liability”: Ghana] [“under the article [Expedited Preservation of Computer Data”: Jamaica], such legislative and other measures as may be necessary to:

(a) ensure that such expeditious preservation of traffic data is available [“possible”: Russian Federation] regardless of whether one or more service providers were [“are”: Jamaica] involved in the transmission of that communication; and

(b) ensure the expeditious disclosure to the [“State”: Jamaica] Party’s competent authority [“competent authorities of the State Party”: Russian Federation], or a person designated by that authority, of a sufficient amount of traffic data to enable the [“State”: Jamaica] Party to identify the service providers and the path through which the communication [“indicated information”: Russian Federation] was transmitted.

The powers and procedures referred to in this article shall be subject to articles [18 and 19] [14 and 15] [31 and 32] [“on scope of procedural measures, and conditions and safeguards”: Ghana] [“Articles (Scope of Procedural Provisions & Conditions and Safeguards”: Jamaica).

(Brazil, Colombia, Ghana, Jamaica on behalf of the CARICOM, Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan)

Source: Council of Europe Convention on Cybercrime, article 17.

Proposal 2

In respect of traffic data that is to be preserved under the previous article:

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

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

(Canada)

H. Production order

Proposal 1

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 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 [the articles on scope of procedural measures, and conditions and safeguards].

(Brazil)

Source: Council of Europe Convention on Cybercrime, article 18, as well as the proposal by Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan, with modifications.

Proposal 2

Each State Party shall adopt the necessary measures to empower its domestic competent authorities to order 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.

(Canada)

Proposal 3

1. Each [“State”: Jamaica] 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.”: Jamaica] to order:

   (a) a person [“including a legal person.”: Jamaica] in its territory to submit specified [delete: Jamaica] computer data in that person’s possession or control [delete: Jamaica], 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 [“State”: Jamaica] Party to submit subscriber information relating to such services in that service provider’s possession or control.

2. The powers and procedures referred to in this article shall be [“subject to the articles on scope of procedural measures, and conditions and safeguards”: Colombia, Switzerland] [“established in accordance with Articles (Scope of procedural provisions and Conditions & Safeguards)”: Jamaica].

3. For the purpose of this article, the term “subscriber information” means [“shall mean”: Jamaica] any information contained in the form of computer data or any other form that is [delete: Jamaica] held by a service provider, relating to subscribers of [“to”: Jamaica] its services other than traffic or content data and by [“on the basis of”: Jamaica] which can be established [“it is possible to establish”: Jamaica]:

94/116 V.22-03252
(a) the type of [“information and”: Jamaica] communication service used, the technical provisions taken thereto [delete: Jamaica] and the period of service;

(b) the subscriber’s identity, postal or geographic address [“addresses”: Jamaica], telephone and other access number [“numbers”: Jamaica], 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”: Colombia, Switzerland] [“information relating to the location of information and telecommunications equipment that has a bearing on the service agreement or arrangement”: Jamaica].

(Colombia, Jamaica on behalf of the CARICOM, Switzerland)

Source: Council of Europe Convention on Cybercrime, article 18.

Proposal 4

1. Each State Party shall adopt 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 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 14 and 15.

   (European Union and its member States)

Proposal 5

1. Each 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 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 relating to such services in that service provider’s possession or control.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the production order for the computer data or subscriber information shall only be obtained by a relevant Competent Authority under the supervision of an independent supervisory entity such as a Judicial Authority. Such measures shall ensure that it is a requirement for the Competent Authority to demonstrate to the satisfaction of the independent Supervisory Authority that there are reasonable grounds to believe that the computer data or subscriber information related to a person under investigation is reasonably required for the purposes of a specific criminal investigations.

3. For the purpose of paragraph 2, the Competent Authority shall

   (a) explain to the independent Supervisory Authority why the Competent Authority believes the computer data or subscriber information sought, will be available to

   (i) The person in control or possession of the computer data or computer system or
(ii) A relevant service provider

(b) Identify and explain with specificity the type of computer data or subscriber information being sought

(c) Indicate what measures shall be taken to ensure that the subscriber information or computer data will be procured

(i) Whilst maintaining the privacy of other users, customers and third parties, and

(ii) Without the disclosure of the subscriber information or computer data of any party not part of the investigation

4. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the independent supervisory authority may grant a production order under paragraph 2 if it is satisfied that

(a) The information requested is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

(b) Measures shall be taken to ensure that the order is executed whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation and

(c) The investigation may be frustrated or seriously prejudiced unless the production of the information is permitted.

5. The powers and procedures referred to in this article shall be subject to Articles 23 and 24.

6. 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.

(Ghana)

Proposal 6

Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a [or otherwise compel a natural or legal: El Salvador] 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.

(El Salvador, Malaysia, United States)

Proposal 7

1. For the purposes set out in article 31, paragraph 1, of this Convention, each State 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 provide specified electronic information in that person’s possession or control;
(b) A service provider offering its services in the territory of that State party to submit subscriber information in that service provider’s possession or control.

2. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

3. For the purposes 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 service used, the technical provisions taken thereto and the period of service;

(b) The subscriber’s identity, postal or other 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.

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

Proposal 8

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 relating to such services in that service provider’s possession or control.

   (c) The powers and procedures referred to in this article shall be subject to human rights safeguards.

2. 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.

   (United Kingdom)
I. Search and seizure of information stored or processed electronically or stored computer data\(^\text{15}\)

Proposal 1

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 its territory or under its own jurisdiction, 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 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.

\((\text{Brazil})\)

Source: China and Russia’s proposal, with modifications to Council of Europe Convention on Cybercrime, article 19.

Proposal 2

1. Each State Party shall adopt the necessary measures to empower its domestic 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 State Party shall adopt the necessary measures to enable its domestic competent authorities to expeditiously extend the search or similar accessing to the

\(^{15}\) Note by the Secretariat: the submissions received used either of the following titles: (1) information stored or processed electronically; or (2) stored computer data.
other system where they have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the system.

3. Each State Party shall adopt the necessary measures to empower its domestic competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures 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; and
   (d) render inaccessible or remove those computer data in the accessed computer system.

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

(Canada)

Proposal 3

1. Each [“State”: European Union and its member States, Jamaica, South Africa] Party shall adopt such legislative and other [delete: European Union and its member States] 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.”: Jamaica] to search or similarly access:

   (a) [“information and communications technologies,”: South Africa] a computer system [“information and communication technology system”: Jamaica] 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”: European Union and its member States, Jamaica, South Africa] Party shall adopt such legislative and other [delete: European Union and its member States] measures as may be necessary to ensure that where its authorities search or similarly access [“any information and communications technologies,”: South Africa] a specific computer system or part of it, pursuant to paragraph 1(a), and have [“reasonable”: Jamaica] grounds to believe that the data sought is stored in another [“information and communications technologies or components forming part of such technologies,”: South Africa] computer system or part of it in its territory, and such data is 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 [State: European Union and its member States, Jamaica] Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities [“where applicable with the assistance or in the presence of the authorized officers of the foreign [“other State Party”: South Africa] 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 [“information and communications technologies or components forming part of such technologies,”: South Africa] a computer system or part of it or a computer-data storage medium;
   (b) make and retain a copy of those computer data;
(c) [“preserve”: India] maintain the integrity of the relevant stored computer data [“computer data”: India];

(d) render inaccessible or remove those computer data in the accessed computer system [“or information and communications technologies”: South Africa] [delete subitem: India].

4. Each [State: European Union and its member States, Jamaica] 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 information and communications technologies or components forming part of such technologies,”: South Africa] a [“the”: India, Jamaica] 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 [“1, 2 and 3”: Jamaica].

[Additional two paragraphs: Ghana]

- Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to be accompanied by an authorized person and is entitled, with the assistance of that person to enable the undertaking of the measures referred to in paragraphs 1, 2 and 3.

- Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize any computer, electronic record, program, information, document, or thing in executing a warrant under its domestic laws if the competent authority has reasonable grounds to believe that any of the offences established in accordance with [the relevant articles] of this convention has been or is about to be committed.]

5. The powers and procedures referred to in this article shall be subject to Articles [14 and 15] [“human rights safeguards”: United Kingdom] [delete subparagraph: India] [“(Scope of Procedural Provisions & Conditions & Safeguards)”; Jamaica].

(Colombia, European Union and its member States, Ghana, India, Jamaica on behalf of the CARICOM, South Africa, Switzerland, United Kingdom)

Source: Council of Europe Convention on Cybercrime, article 19.

Proposal 4

1. Each State 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 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 grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is 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 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 and 2.

(El Salvador, United States)

Proposal 5

1. Each State party shall adopt such legislative and other measures as may be necessary 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 territory or under the 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 1–3 of this article.

5. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

(Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan)
J. Real-time collection of traffic data

Proposal 1

1. Each ["State": Jamaica] 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."]; Jamaica] 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, ["in accordance with its domestic law, "; Jamaica] 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 ["State": Jamaica] Party shall adopt such legislative and other measures as may be necessary to oblige ["require": Jamaica] 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.

(Brazil, Colombia, India, Jamaica on behalf of CARICOM)

4. The powers and procedures referred to in this article shall be subject to articles ["18 and 19"] ["14 and 15"] ["(Scope of Procedural Provisions & Conditions & Safeguards")].

(Brazil, Colombia, Jamaica on behalf of CARICOM)

Source: Council of Europe Convention on Cybercrime, article 20.

Proposal 2

Each State 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 in the territory of that State Party; and

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

collect or record through the application of technical means in the territory of that State Party; or cooperate with and assist the competent authorities in the collection or recording of traffic data, in real time, associated with specific communications in its territory, transmitted by means of a computer system.

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 in that territory.

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

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. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the power under this article shall only be obtained by a relevant Competent Authority under the supervision of an independent supervisory entity such as a Judicial Authority. Such measures shall ensure that it is a requirement for the Competent Authority to demonstrate to the satisfaction of the independent Supervisory Authority that there are reasonable grounds to believe that the traffic data related to a person under investigation is reasonably required for the purposes of a specific criminal investigations.

3. For the purpose of paragraph 2, the Competent Authority shall

   (a) explain to the independent Supervisory Authority why the Competent Authority believes traffic data sought, will be available to

      (i) the person in control or possession of the computer system or

      (ii) a service provider

   (b) Identify and explain with specificity the type of traffic data being sought;

   (c) Identify and explain with specificity the offences in respect of which the power under this article is sought;

   (d) Indicate what measures shall be taken to ensure that traffic data will be procured

      (i) Whilst maintaining the privacy of other users, customers and third parties,

      and

      (ii) Without the disclosure of traffic data of any party not part of the investigation

4. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the independent supervisory authority may grant the power of real-time collection of traffic data if the independent supervisory authority is satisfied that

   (a) The extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

   (b) Measures shall be taken to ensure that the power is executed whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation and

   (c) The investigation may be frustrated or seriously prejudiced unless the power for real-time collection of traffic data is permitted.

5. 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.

6. 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.

7. The powers and procedures referred to in this article shall be subject to Articles 23 and 24.

(Ghana)

Proposal 4

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

   (a) Collect or record, employing technical means for this purpose, the traffic data associated with ICT use in the territory of that State party; and

   (b) Oblige service providers, to the extent that they possess the technical capacity to do so:

      (i) To collect or record traffic data in the territory of that State party, employing technical means for this purpose; or

      (ii) To cooperate with and assist the competent authorities of that State party in collecting or recording in real time the traffic data associated with specified information in the territory of that State party.

2. Where a State party, owing to the long-standing principles of its domestic legal system, cannot adopt the measures provided for in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of the traffic data in its territory through the application of technical means in that territory.

3. Each State party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the exercise 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 the provisions of articles 31 and 32 of this Convention.

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

Proposal 5

1. Each State 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 information and communications technologies or a computer system.

   (South Africa)
Proposal 6

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

(United States)

K. Interception of content data

Proposal 1

1. Each [“State”: Jamaica] Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious [“criminal”: Jamaica] 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, “: Jamaica] to:

   (a) collect or record [“or store”: Jamaica] 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 [“State”: Jamaica] Party, due to the established principles of its domestic legal system [“in accordance with its domestic law,”: Jamaica], 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 [“State”: Jamaica] 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.

(Brazil, Colombia, India, Jamaica on behalf of the CARICOM)
4. The powers and procedures referred to in this article shall be subject to articles [“18 and 19”] [“14 and 15”] [“(Scope of Procedural Provisions & Conditions and Safeguards)”].

(Brazil, Colombia, Jamaica on behalf of the CARICOM)

Source: Council of Europe Convention on Cybercrime, article 21.

Proposal 2

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

(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, to: collect or record through the application of technical means in the territory of that Party; or cooperate with and assist the competent authorities in the collection or recording of content data, in real time, associated with specific communications in its territory transmitted by means of a computer system.

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 in that territory.

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

(El Salvador)

Proposal 3

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 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 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. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the power under this article shall only be obtained by a relevant Competent Authority under the supervision of an independent supervisory entity such as a Judicial Authority. Such measures shall ensure that it is a requirement for the Competent Authority to demonstrate to the satisfaction of the independent Supervisory Authority that there are reasonable grounds to authorize the interception of content data related to or connected with person or premises under criminal investigations for one of the following purposes:

(a) The interests of national security

(b) The prevention or detection of a serious offence
(c) In the interests of the economic well-being of the citizenry, so far as those interests are also relevant to the interests of national security; or
(d) To give effect to a mutual legal assistance requests

3. For the purpose of paragraph 2, the Competent Authority shall
   (a) explain to the independent Supervisory Authority why the Competent Authority believes the content sought, will be available to
      (i) the person in control or possession of the computer system
      (ii) a service provider
   (b) Identify and explain the type of content data suspected to be found on the computer system or in the possession or control of the service provider
   (c) Identify and explain with specificity the offences in respect of which the power under this article is sought;
   (d) Indicate what measures shall be taken to ensure that the content data will be procured
      (i) Whilst maintaining the privacy of other users, customers and third parties, and
      (ii) Without the disclosure of traffic data of any party not part of the investigation

4. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the independent supervisory authority may grant the power of interception of content data if the independent supervisory authority is satisfied that
   (a) The extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;
   (b) Measures shall be taken to ensure that the power of interception of the content data is executed whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation and
   (c) The investigation may be frustrated or seriously prejudiced unless the interception is permitted.

5. 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.

6. 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.

7. The powers and procedures referred to in this article shall be subject to Articles 23 and 24.

(Ghana)

Proposal 4

1. Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
   (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 information and communications technologies 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 27 and 28.

(South Africa)

Proposal 5

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

   (a) collect or record through the application of technical means on the territory of that State 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 State 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 State 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 State Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(United States)

L. Collection of information/content and meta data transmitted by means of information and communications technologies

Proposal 1

Collection of content and meta data

1. Each Party shall adopt such legislative and other measures as may be necessary to provide meta data expeditiously without the need of MLAT. The service provider who has such meta data 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. Mechanism for such expeditious data sharing will be developed under this convention.

(India)

Proposal 2

Collection of information transmitted by means of information and communications technologies

1. In order to counter the offences covered by this Convention and established as such under its domestic legislation, each State party shall adopt such legislative and other measures as are necessary to empower its competent authorities to:

   (a) Collect or record, through the application of technical means, in the territory of that State party, information transmitted by means of ICT; and

   (b) Oblige a service provider, to the extent that it possesses the technical capacity to do so:

   (i) To collect or record, through the application of technical means in the territory of that State party, electronic information which includes data on content and is transmitted by means of ICT; or

   (ii) To cooperate with and assist the competent authorities of that State party in real time collection or recording of electronic information which includes data on content and is transmitted by means of ICT in the territory of that State party.

2. Where a State party, owing to the long-established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of electronic information which includes data on content and is transmitted by means of ICT in its territory through the application of technical means in that territory.

3. Each State party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the exercise 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 the provisions of articles 31 and 32 of this Convention.

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

M. Retention of data

Proposal 1

1. Each Party shall adopt such legislative and other measures as may be necessary, to ensure that a service provider within its territory shall retain

   (a) subscriber information for at least six (6) years;

   (b) traffic data for a period of twelve (12) months.

2. The powers and procedures referred to in this article shall be subject to [the articles on scope of procedural measures, and conditions and safeguards].

3. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to under this Article that Party may reserve the right not to apply these measures. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to under this Article.

(Ghana)
N. Admission of digital evidence

Proposal 1

Digital evidence derived or extracted from devices, equipment, electronic media, information systems, computer programs or any ICT shall have the probative value of material forensic evidence in criminal evidence when such digital evidence meets the technical conditions under the laws of the States parties.

(Egypt)

O. Freezing, seizure and confiscation

Proposal 1

1. Each State Party shall take, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable confiscation of:
   
   (a) Proceeds of crime derived from offences established in accordance with this Convention or property the value of which corresponds to that of such proceeds;
   
   (b) Property, equipment or other instrumentalities used in or destined for use in offences established in accordance with this Convention.

2. Each State Party shall take such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

3. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.

4. If such proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

5. If such proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

6. Income or other benefits derived from such proceeds of crime, from property into which such proceeds of crime have been transformed or converted or from property with which such proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

7. For the purpose of this article and article 55, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

8. States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of such alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the fundamental principles of their domestic law and with the nature of judicial and other proceedings.

9. The provisions of this article shall not be so construed as to prejudice the rights of bona fide third parties.

10. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.
Proposal 2

1. States Parties [“Each Party”: Ghana] shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:

   (a) Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

   (b) Property, equipment or other instrumentalities used in or destined for use in offences covered by this Convention.

2. States Parties [“Each Party”: Ghana] shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any of the [delete: Ghana, United States] items referred to in the preceding paragraph [“paragraph 3 of this article”: Ghana; “paragraph 1 of this article”: United States] for the purpose of eventual confiscation.

3. If proceeds of crime have been transformed or converted, in full or in part [“in part or in full”: Ghana, United States], into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

4. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

5. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same way [“manner”: Ghana, United States] and to the same extent as proceeds of crime.

6. [“For the purposes of this article,”: Ghana] [“For the purposes of this article and article [international cooperation for purposes of confiscation] of this Convention,”: United States ] Each [“State”: El Salvador, United States] Party shall empower its courts or other competent authorities to [in: United States] order that bank, financial or commercial records be made available or be seized. States Parties [“Member States”: Ghana] shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

7. States Parties [“Each Party”: Ghana] may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings.

8. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

9. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party [“Member State”: Ghana].

(El Salvador, Ghana, United States)

Source: Organized Crime Convention, article 12, with modification.

Proposal 3

1. Notwithstanding the fact that the provisions of this article it shall not be so construed as to prejudice the rights of bona fide third parties and that nothing
contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

2. The provisions of this article shall not be so construed as to prejudice the rights of bona fide third parties.

3. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

4. Each State Party shall take, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable confiscation of:

   (a) Proceeds of crime derived from offences caused by the use of information and communication technologies established in accordance with this Convention or property the value of which corresponds to that of such proceeds and to the benefit of the affected State Party;

   (b) Property, equipment or other instrumentalities including the use of information and communications technologies used in or destined for use in offences established in accordance with this Convention.

4. Each State Party shall take such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

5. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.

6. If such proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

7. If such proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

8. Income or other benefits derived from such proceeds of crime, from property into which such proceeds of crime have been transformed or converted or from property with which such proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

9. For the purpose of this article and article----[on international cooperation] of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

10. States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of such alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the fundamental principles of their domestic law and with the nature of judicial and other proceedings.

(South Africa)
P. Disposal of confiscated proceeds of crime or property

Proposal 1

1. Proceeds of crime or property confiscated by a State Party pursuant to the article on confiscation and seizure and [the article on international cooperation for the purposes of confiscation] [“article 33, paragraph 3,”: South Africa] of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures.

2. When acting on the request made by another State Party in accordance with article [the article on international cooperation for the purposes of confiscation] [article 39: South Africa] of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their legitimate owners.

3. When acting on the request made by another State Party in accordance with the article on confiscation and seizure and [the article on international cooperation for the purposes of confiscation] [“article 41”: South Africa] of this Convention, a State Party may [“, after due consideration has been given to compensation to victims,”: El Salvador, United States] give special consideration to concluding agreements on or arrangements on:
   
   (a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with [the article on technical assistance] [article -: South Africa] of this Convention and to intergovernmental bodies specializing in the fight against cybercrime [“organized crime”: South Africa];

   (b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

   (El Salvador, South Africa, United States)

Source: Organized Crime Convention, article 14.

Q. Special investigative techniques

Proposal 1

1. In order to combat or counter the use of information and communications technologies for criminal purposes effectively, each State Party shall, to the extent permitted by the basic principles of its domestic legal system and in accordance with the conditions prescribed by its domestic law, take such measures as may be necessary, within its means, to allow for special investigative techniques, such as electronic or other forms of surveillance and undercover operations, within its territory, and to allow for the admissibility in court of evidence derived therefrom, without compromising the cyber security threat and confidentiality of the intelligence of each State Party.

2. For the purpose of investigating the offences involving the use of information and communications technologies covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States, respect of fundamental human rights and freedoms and shall be carried out strictly in accordance with the terms of those agreements or arrangements.
3. In the absence of an agreement or arrangement as set forth in paragraph 2 of this article, decisions to use such special investigative techniques at the international level shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the States Parties concerned.

(South Africa)

Source: Convention against Corruption, article 50, and Organized Crime Convention, article 20, with modifications.

R. Establishment of criminal record

Proposal 1

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence [covered by this Convention: El Salvador, United States] [caused by the use of information and communications technologies established in accordance with this Convention: South Africa].

(El Salvador, South Africa, United States)

Source: Convention against Corruption, article 41, and Organized Crime Convention, article 22, with modifications.

S. Protection of witnesses

Proposal 1

1. Each State Party shall take appropriate measures within its means to provide effective protection from potential retaliation or intimidation for witnesses in criminal proceedings who give testimony concerning offences covered by this Convention and, as appropriate, for their relatives and other persons close to them.

2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:

   (a) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where appropriate, non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of such persons;

   (b) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means.

3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.

4. The provisions of this article shall also apply to victims insofar as they are witnesses.

(El Salvador, United States)

Source: Organized Crime Convention, article 24.

Proposal 2

Each State party shall consider adopting such legislative measures as may be necessary to provide effective protection for the following:
(a) Persons who, in good faith and on reasonable grounds, provide information relating to illegal acts covered by articles 6–28 of this Convention or otherwise cooperate with investigating or judicial authorities;

(b) Witnesses who give testimony concerning illegal acts covered by articles 6–28 of this Convention, as well as victims;

(c) Where appropriate, family members of the persons referred to in subparagraphs (a) and (b) of this article.

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

T. Assistance and protection of victims

Proposal 1

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences covered by ["established in accordance with [the articles on criminalization] of": European Union and its member States] this Convention [", in particular in cases of threat of retaliation or intimidation": El Salvador, United States].

2. Each State Party shall establish appropriate procedures to provide access to compensation ["and restitution": El Salvador, United States] for victims of offences covered by ["established in accordance with [the articles on criminalization] of": European Union and its member States ] this Convention.

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

(El Salvador, European Union and its member States, United States)

Source: Organized Crime Convention, article 24, and Convention against Corruption, article 32.

Proposal 2

Rights of the victim

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.

(Malaysia)

U. Measures to enhance cooperation with law enforcement authorities

Proposal 1

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in [“offenses established by this convention”: United States] [“organized criminal groups”: El Salvador, South Africa]:

(a) To supply information useful to competent authorities for investigative and evidentiary purposes on such matters as:

(i) The identity, nature, composition, structure, location or activities of [“persons participating in offenses established by this convention”: United States] [“organized criminal groups”: El Salvador, South Africa];
(ii) Links, including international links, with other persons participating in offenses established by this convention;

(iii) Offences that persons participating in offenses established in this convention have committed or may commit;

(b) To provide factual, concrete help to competent authorities that may contribute to depriving [“persons participating in offenses established by this convention”: United States] [“organized criminal groups”: El Salvador, South Africa] of their resources or of the proceeds of crime.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

4. Protection of such persons shall be as provided for in the article on protection of witnesses of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

(El Salvador, South Africa, United States)

Source: Organized Crime Convention, article 26.