UK contribution on General Provisions, Criminalisation and Procedural Measures and Law Enforcement

The UK is pleased to submit to the AHC an initial contribution encompassing textual suggestions and general comments on the requested chapters.

Chapter – General Provisions

Article 1

Purpose

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

Article 2

Definitions

For the purposes of this Convention

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

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

“service provider" means:

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

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

Article 3

Scope of application

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

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

Article 4

Protection of human rights

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

Additional comments

The UK believes it may also be appropriate for the General Provisions chapter to address how this convention relates to, and complements, other UN criminal justice instruments, and to include a commitment to mainstream a gender perspective in implementing the Convention's provisions.

Chapter – Criminalisation

Cyber-dependent offences

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

Article 5

Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 6

Illegal Interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 7

Data interference

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

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

Article 8

System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 9

Misuse of devices

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

    c. the production, sale, procurement for use, import, distribution or otherwise making available of:

        i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with sections ;

        ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

    with intent that it be used for the purpose of committing any of the offences established in the other four Articles in this section; and

    d. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the other four Articles in this section. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles relating to illegal access, illegal interception, data interference and system interference, such as for the authorised testing or protection of a computer system.

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

Cyber-enabled offences

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

Article 10

Fraud

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

a. fraud by false representation,
b. fraud by failing to disclose information,
c. fraud by abuse of position, with fraudulent or dishonest intent to cause a loss to another or make a gain in money or other property for another person.

Article 11

Offences related to online Child Sexual Exploitation and Abuse (CSEA), including CSEA material and online grooming

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

    a. producing CSEA material for the purpose of its distribution through a computer system;
    b. offering or making available CSEA material through a computer system;
    c. distributing or transmitting CSEA material through a computer system;
    d. procuring CSEA material through a computer system for oneself or for another person;
    e. possessing CSEA material in a computer system or on a computer-data storage medium.
    f. viewing CSEA material in a computer system or on a computer-data storage

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

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

c. realistic images representing a minor engaged in real or simulated sexually explicit conduct.
d. any depiction of a minor's sexual organs for primarily sexual purposes

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c

Article 12

Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the World Intellectual Property Organisation (WIPO)Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article

Article 13

Attempts, aiding & abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with [this Convention] with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with this Convention.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 14

Prosecution, adjudication and sanctions

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

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

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

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

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

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

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

Article 15

Jurisdiction

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

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

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

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

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

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

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

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

Additional Comments

The UK believes that the use of digital technology to communicate with a minor where that communication is sexual in nature, or is made with the intention of encouraging the minor to engage in sexual communication or activity, and

where that communication is made for the purpose of obtaining sexual gratification, should be criminalised, and we will provide text on this during negotiations.

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

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

Chapter – Procedural measures and law enforcement

Article 16

Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights law, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 17

Scope of procedural provisions, including the wider use of procedural law for all offences

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 the offences defined inf this Convention;
    b. other criminal offences committed by means of a computer system; and
    c. the collection of evidence in electronic form of a criminal offence.

Article 18

Expedited preservation

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to human rights safeguards.

Article 19

Production order

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

    a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
    b. a service provider offering its services in the territory of the Party to submit subscriber information 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.

Article 20

Search and seizure of stored computer data

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

    a. a computer system or part of it and computer data stored therein; and
    b. a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought 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 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 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.
5. The powers and procedures referred to in this article shall be subject to human rights safeguards.