Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Elaboration of a convention on cybercrime / countering the use of information and communications technologies for criminal purposes – 2nd formal session 30 May–10 June 2022

Switzerland's submission relating to provisions on criminalization, general provisions and provisions on procedural measures and law enforcement

The present document outlines Switzerland's view and proposals on provisions on criminalization, general provisions and provisions on procedural measures and law enforcement, to be discussed at the AHC second formal session from 30 May–10 June 2022.

These concrete proposals are often based on or inspired by existing provisions of International Criminal Law treaties and are presented in light of such existing international legal instruments relevant to the elaboration of the future UN cybercrime treaty. The proposals made are to be understood as a starting point in view of the upcoming discussions. We hope that these proposals will contribute to a fruitful and constructive discussion at the AHC's next meetings. The present submission may also provide some guidance regarding the direction and goals that, in our view, the negotiations should be aimed at during the meetings.

1. General remarks

A future UN convention on countering cybercrime / the use of ICTs for criminal purposes should be agreed by consensus, be universally acceptable, effective and geared toward its implementation and use by law enforcement authorities ("user-friendly"). Importantly, the future convention should facilitate and expedite States' and their relevant authorities' understanding of what constitutes cybercrime. Respect and protection of human rights obligations should be mainstreamed in the convention ("human rights-based approach"). The future convention should also take into account gender aspects.

In order to meet these requirements, the future convention should

- be sharply focused on a limited and clearly defined number of cyber-dependent crimes and an even more limited number of cyber-enabled crimes;
- be focused on behaviours and not on evolving technologies, with a view to being future proof and to limiting the need to constantly amend the convention in order to reflect new technological developments;
- make effective use of existing legal instruments (incl. well established terminologies) and related practice, reflective of existing consensus among Member States;
- be made up of, as far as possible, clear and concise provisions, while also taking into account the sometimes complex issues to be dealt with.

General remark on collection and aggregation of traffic data
The future convention needs robust safeguards that prevent negative impact on the right to privacy, freedom of expression, freedom of association, and other human rights.

2. Specific text proposals

2.1 General provisions

Statement of purpose
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

Respect and protection of human rights and fundamental freedoms
States Parties must carry out their obligations under this Convention in a manner consistent with their obligations under international human rights law.

Use of terms
"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.

Scope of application
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.

2.2 Provisions on criminalization

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

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

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

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

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

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

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

a. the production, sale, procurement for use, import, distribution or otherwise making available of:
    i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the provisions on illegal access, illegal interception, data interference or system interference of this Convention;
    ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the provisions on illegal access, illegal interception, data interference or system interference of this Convention; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in accordance with the provisions on illegal access, illegal interception, data interference or system interference of this Convention . A Party may require that a number of such items be possessed before criminal liability attaches.

[2] This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with the provisions on illegal access, illegal interception, data interference or system interference of this Convention, such as for the 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.

<u>b. Computer-related offences</u>

Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Computer-related fraud
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data,
b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

c. Content-related offences

Offences related to child sexual exploitation and abuse material
[1] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

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

[2] For the purpose of paragraph 1 above, the term "child sexual exploitation and abuse material" shall include material that visually depicts:

a. a minor engaged in sexually explicit conduct;
b. a person appearing to be a minor engaged in sexually explicit conduct;
c. realistic images representing a minor engaged in sexually explicit conduct.

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

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

d. Ancillary liability and sanctions

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

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

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

Liability of legal persons

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

a. a power of representation of the legal person;
b. an authority to take decisions on behalf of the legal person;
c. an authority to exercise control within the legal person.

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

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

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

Sanctions and measures

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

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

2.3 Provisions on procedural measures and law enforcement

Section 1

a. Common provisions

Scope of procedural provisions

[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] 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 provisions on criminalization 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

a. Each Party may reserve the right to apply measures on real-time collection of traffic data 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 measures on interception of content data. Each Party shall consider restricting such a reservation to enable the broadest application of measures on real-time collection of traffic data.
b. 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 measures on real-time collection of traffic data and on interception of content data to communications being transmitted within a computer system of a service provider, which system:
   i. is being operated for the benefit of a closed group of users, and
   ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

that 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 measures on real-time collection of traffic data and on interception of content data.

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 and regional human rights instruments, and which shall incorporate the principle of proportionality.

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

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

<u>b. Expedited preservation of stored computer data</u>

Expedited preservation of stored computer data

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

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

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

[4] The powers and procedures referred to in this article shall be subject to the provisions on the scope of procedural provisions and on conditions and safeguards of this Convention.

c. Production order

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.

[2] The powers and procedures referred to in this article shall be subject to the provisions on the scope of procedural provisions and on conditions and safeguards of this Convention.

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

a. the type of communication service used, the technical provisions taken thereto and the period of service;
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

d. Search and seizure of stored computer data

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 the provisions on the scope of procedural provisions and on conditions and safeguards of this Convention..

Section 2

e. Jurisdiction

Jurisdiction

[1] Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with 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.