Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Elaboration of a convention on countering the use of information and communications technologies for criminal purposes

Switzerland's view on the objectives, scope and structure

Information and communication technologies (ICTs) have deeply impacted our society, offering opportunities for development on a social, cultural, and economic level, but also a ground for activities with criminal purposes that take place in cyberspace. As our world becomes increasingly digitalized, cybercrime is on the rise. Through Resolution A/Res/74/247, the UN General Assembly established an open-ended ad hoc intergovernmental committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. The present document outlines Switzerland's view on the objectives, the scope and the structure of this instrument.

1. Objectives:

For Switzerland, the **overarching goal** of a United Nations convention countering the use of ICTs for criminal purposes is **to protect ICT users, so that they can use ICTs freely and enjoy their benefits**. The global and open nature of ICTs is indeed a driving force in accelerating progress towards social and economic development. The aim of the convention is therefore the safety of users, which shall not hamper their freedom to use ICTs. Users must be able to exercise their human rights and fundamental freedoms online, thereby realizing the full potential of an inclusive digitized world. The convention should therefore be a step further to ensure free, trusted and safe ICTs.

A United Nations convention can help us attain this overarching goal. To do so, the convention should provide for a **coordinated approach in the fight against cybercrime**. Because of the inherently transnational nature of ICTs, cybercrimes are likely to involve perpetrators and victims based in multiple States. International cooperation is therefore key to ensure the best level of protection against cybercrimes. The convention should aim to create a **common understanding** of what constitute criminal offences in the context of ICTs, and which offences should be punishable under national law. This common understanding is the first building block to enabling any sort of cooperation. On the basis of this shared understanding and vocabulary, the convention should aim to create the **framework for an effective international cooperation** to protect ICT users and to obtain justice for the victims of cybercrime.

A coordinated approach to fight cybercrime at the global level can only be achieved through an **inclusive process**. All UN Member States should be able to engage meaningfully: they should have the opportunity to present their views on the convention and discuss the views presented by others during the substantive meetings of the Ad Hoc Committee. The Ad Hoc Committee should strive for **consensus, whenever possible**.

Cybercrime is transnational, but also inherently involving non-state actors. If we want a convention **fit for purpose, every voice needs to be heard** during the elaboration process. Including all stakeholders – among which relevant non-governmental organizations, civil society organizations, academic institutions and the private sector – in each coordinated step of the elaboration is key to ensure that the convention fulfil its objectives.[1]

2. Scope:

International law applies to cyberspace. The future convention will not exist in a vacuum, nor will it empty previous international agreement of their significance. It is our conviction that this convention must **build upon and should reinforce the current legal regime**. It should be designed to complement the initiatives already undertaken by the international community, and to rely on synergies to effectively tackle cybercrime.

As the convention will be a criminal law treaty, it should build on and respect international criminal law. Global tools to address the issue of cybercriminality already exist. Along with the United Nations **Convention against Transnational Organized Crime** (UNTOC), the **Budapest Convention** has been a standard by which countries from around the globe, including Switzerland, have been modernizing their cybercrime laws. It is also an important baseline for international cooperation in the Internet Age. A UN convention should build upon this experience. The work of the Committee should be guided by the work of other groups and fora, including the Expert Group to Conduct a Comprehensive Study on Cybercrime.

The convention must adequately reflect, safeguard and reinforce **human rights law**. As cybercrime poses a threat to individuals' human rights, efforts to address it need to protect, not undermine, these rights. The same rights that individuals have offline must also be protected online. Measures undertaken to combat cybercrime must be consistent with international human rights law.

3. Structure:

Switzerland considers that a promising and efficient approach to concretize the objectives mentioned above is to follow the systematics of existing International Criminal Law Instruments negotiated in the context of the UN. The convention could therefore be structured as follows:

a) General provisions
b) Preventive measures
c) Criminalization and law enforcement
d) International cooperation
e) Technical assistance and information exchange
f) Mechanisms for implementation
g) Final provisions

- Switzerland considers that there is **no need to duplicate** offences which are already covered by specific treaties (for example corruption, trafficking, terrorism, etc.) simply out of the reason that they may (also) be committed via ICTs. Instead, the convention should focus on crimes which are specific to cyberspace. A broad listing of offences, although all of them may be committed by means of computer systems, entails the risk of contradiction and should be avoided.

- Content related offences should be kept at a low number and always checked with regard to their **added value**.

[1] In accordance with A/Res/75/282, paragraphs 9-10.

- Switzerland emphasizes the need and importance of **procedural guarantees** that ensure the **legality and fairness of proceedings** and the **rights of persons affected**, regarding in particular mutual legal assistance, the exchange of information and extradition under the conditions set by the concerned States. The **right to privacy** must be fully guaranteed. An adequate level regarding the **protection of personal data** must be ensured.

- Adequate conditions and safeguards must be considered and introduced, in particular regarding maintaining and **strengthening human rights**, including the principle of **non-discrimination**.