

20 April 2022

English only

---

**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

**Proposals on objectives and scope of the Comprehensive  
International Convention on Countering the Use of  
Information and Communications Technologies for  
Criminal Purposes**

**Note by the Secretariat****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. It is indicative in nature, with a view to providing guidance for the future work of the Ad Hoc Committee, and contains proposals on the objectives and scope of the convention.

**II. Proposal on the objectives of the convention**

2. The objectives of the convention are to:
- Promote and strengthen measures to [counter] [prevent and combat]<sup>1</sup> [the use of information and communications technologies for criminal purposes] [cybercrime],<sup>2</sup> while protecting users of information and communications technologies from such crime;
  - Promote, facilitate and strengthen international cooperation in [countering] [preventing and combating] [the use of information and communications technologies for criminal purposes] [cybercrime];

---

<sup>1</sup> The terms “counter” and “prevent and combat” have both been included as options, pending further discussion and a final decision on the use of terms.

<sup>2</sup> The terms “use of information and communications technologies for criminal purposes” and “cybercrime” have both been included as options, pending further discussion and a final decision on the use of terms.



- Provide practical tools to enhance technical assistance among States parties, to build the capacity of national authorities to [counter] [prevent and combat] [the use of information and communications technologies for criminal purposes] [cybercrime], in particular for the benefit of developing countries, and to strengthen measures to promote the exchange of information, specialized knowledge, experiences and good practices.

### III. Proposal on the scope of the convention

#### Scope of application

3. The future convention shall apply to [countering] [preventing and combating] [the use of information and communications technologies for criminal purposes] [cybercrime].

#### Elements to include within the scope of the convention

4. Taking into full consideration applicable international instruments and efforts at the national, regional and international levels, the convention is to include provisions<sup>3</sup> on the following:

(a) Ensuring comprehensive protection of human rights and fundamental freedoms, consistent with applicable international obligations;

(b) Ensuring full compliance with the fundamental principles of international law, including the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States;

(c) Providing assistance and protection to victims, especially those from vulnerable groups;

(d) Taking into consideration child- and gender-sensitive issues;

(e) Defining the types of crime that involve [the use of information and communications technologies for criminal purposes] [cybercrime], that should be considered as criminal acts in the legal systems of all States parties;

(f) Establishing criminal liability for the commission of the offences as set out in the convention, as well as accessory and ancillary liability. The liability of legal persons is also to be established;

(g) Providing for criteria to establish jurisdiction over crimes set out in the convention;

(h) Establishing sufficient procedural powers to enable the timely response to, and investigation and prosecution of, the offences set out in the convention;

(i) Developing measures, in particular establishing and strengthening competent authorities, to ensure the preservation, collection, obtaining and sharing of electronic evidence;

(j) Establishing specific measures to deal with the proceeds of offences set out in the convention;<sup>4</sup>

(k) Defining prevention measures,<sup>5</sup> and limiting the risk of [the use of information and communications technologies for criminal purposes] [cybercrime] for individuals, businesses and States parties;

---

<sup>3</sup> The provisions are listed in no particular order.

<sup>4</sup> Some delegations indicated that these measures should include seizure and confiscation of the proceeds of offences, while some other delegations insisted on including seizure, confiscation and return of such proceeds.

<sup>5</sup> Some delegations indicated that such preventive measures are to be limited to the criminal justice level.

(l) Promoting, facilitating and supporting international cooperation, in particular through effective and rapid mutual legal assistance and the establishment of 24/7 contact points, as well as, inter alia, extradition, special investigative techniques and law enforcement cooperation;

(m) Providing tools to enhance technical assistance and capacity-building, in particular for the benefit of developing countries, including for the exchange of information, experiences and good practices, and noting, in particular, the role of the United Nations Office on Drugs and Crime in this regard;

(n) Taking appropriate measures conducive to the optimal implementation of the convention, including through economic development;

(o) Defining clear mechanisms for implementation and other follow-up mechanisms;

(p) Encouraging States parties to take appropriate measures, within their means and in accordance with the fundamental principles of domestic law, to promote the active participation of individuals and groups outside the public sector in [countering] [preventing and combating] [the use of information and communications technologies for criminal purposes] [cybercrime], including in raising public awareness regarding the existence, causes and gravity of, and the threat posed by [the use of information and communications technologies for criminal purposes] [cybercrime].

---