

Comments and proposals of the Islamic Republic of Iran on the provisions of criminalization, the general provisions, and the provisions on procedural measures and law enforcement of the convention on countering the use of ICT for criminal purposes

The Islamic Republic of Iran, considering that the first reading of the sections of the convention on general provisions, criminalization, law enforcement and procedural measures will be conducted during the second session of the Ad hoc Committee to be held from 30 May to 10 June 2022 in Vienna and recalling its comments and proposals presented, *inter alia*, during the first substantive session of the Ad hoc Committee, would like to submit and reaffirm its comments and proposals, as following, regarding the said sections.

The present submission does not prejudice contributions of the Islamic Republic of Iran on the abovementioned sections and any other section of the convention in future and throughout the process of elaboration of the convention. The Islamic Republic of Iran, as it may deem appropriate, may provide concrete proposals or general comments, positions and observations on and in relation to the abovementioned provisions in the course of elaboration of the convention including during the substantive sessions of the Ad hoc Committee.

1. General provisions

- Despite the exceptional opportunities presented by information and communications technologies for development of nations, criminals are exponentially misusing such technologies to carry out illicit activities and realize illegitimate purposes. The *modi operandi* of such criminals are becoming increasingly diversified and sophisticated and the compounded nature of such offences is substantially evolving. Crimes committed via use of ICT often transcend geographical boundaries turning it into an unprecedented pressing challenge for Member States to overcome. As such, a strengthened collective response and cooperation at the international level within a sound international legal framework is more than necessary.
- The *raison d'être* for the establishment of the Ad hoc Committee pursuant to resolution 74/247 was to respond to this urgent need and to elaborate an international legal instrument that supports effective measures at various levels in fighting the use of ICT for criminal purposes. To this end, the general provisions of the convention should stipulate the purposes of the convention and define its purview. As an established practice and given the underlying

importance of compliance with the fundamental principles of international law in preventing and combating crimes committed via use of ICT, a substantive section should also be dedicated to such principles under the general provisions. Defining the terminologies used in the convention under a specific section is essential to ensure common understating of important terms and ultimately of the provisions of the convention.

1.1.Objectives of the convention

- In view of the above, the Islamic Republic of Iran highlights that the convention should aim to strengthen, support and facilitate international cooperation in preventing and combating the use of ICT for criminal purposes including in asset recovery, to strengthen national responses to such crimes and to assist state parties, in particular, developing countries, in fighting these crimes, *inter alia*, through economic development, provision of technical assistance and transfer of technology. In this relation, the challenges and barriers such as unilateral sanctions and underdevelopment that undermine the ability of states to effectively fight the use of ICT for criminal purposes should be addressed in a technical context.
- Due regard should also be had to the responsibility of service providers and other similar entities in cooperating with judicial and law enforcement authorities so as to ensure effective measures in preventing and combating the use of ICT for criminal purposes.
- Whereas a common understanding of the criminal phenomena and its evolving forms is of utmost importance in effectively responding to crimes committed via ICT, the convention should also promote and facilitate the exchange of information, expertise, specialized knowledge, experiences and good practices.
- Such objectives will be well realized by adopting an approach that cherishes a shared future in cyberspace for all Member States with equal opportunities and without discrimination.

1.2.Scope of the Convention

- The convention should have within its purview crimes that are dependent on ICT such as crimes against confidentiality and integrity of ICT systems and data and crimes against ICT infrastructures as well as those enabled by such technologies e.g. insult to religious values, incitement to violence, encouragement to commit homicide, distribution of criminal and obscene content and child sexual exploitation. Nevertheless, crimes enabled by ICT may require a case-by-case approach that considers different factors surrounding various forms of crimes and possible differences in the elements of crime

necessary to establish as offences. Where appropriate, further elements may also be needed to define the ambits of the convention based on the severity or penalties of offences and taking into account whether the offences in question have been perpetrated in more than one state.

1.3. Protection of sovereignty

- The Islamic Republic of Iran reaffirms that specific sections on protection of sovereignty should be included in the general provisions to ensure that efforts and measures in preventing and combating the use of ICT for criminal purposes are consistent and in compliance with the fundamental principles of international law and the principles set forth in the Charter of the United Nations, in particular, sovereignty equality, territorial integrity of states and that of non-intervention. This is an established practice in elaboration of conventions in the field of preventing and combating crimes; as a case in point, the term “protection of sovereignty” has been utilized in the conventions such as the United Nations Convention against Corruption.
- The Islamic Republic of Iran remains circumspect regarding attempts that at variance with this established practice of the international community aim to negate and ignore the essential role of conformity with such principles in fighting crimes.

2. Criminalization

- It is increasingly the case that offenders organize and carry out unlawful activities not only against but through ICT devices. Though criminal acts may be established as offences notwithstanding misuse of ICT or vice-versa, in certain cases the gravity and other factors surrounding the offence requires criminalizing the unlawful act when conducted via use of ICT. This is especially the case when use of ICT intensifies commission of crimes in terms of, *inter alia*, extent of harm it inflicts upon victims. Therefore, in addition to crimes dependent on ICT, crimes enabled by these technologies should be criminalized within the convention. Nonetheless, from a legal standpoint this may require a case-by-case approach since various forms of crime may reflect differentiated elements as well as *actus reus* and *mens rea*. In adopting measures for establishing offences due regard should be had as to the fundamental principles of domestic legal systems.
- Liability of legal persons should also be established to ensure a comprehensive response to criminal activities and to deny offenders of freedom of operation under the veil of legal entities. Such measure should hold legal persons liable

for deliberate or otherwise knowingly involvement in the commission of offences to be established in accordance with the convention.

3. Law enforcement and procedural measures

- Criminals often perpetually and increasingly misuse services provided by private sectors including service providers and social media networking platforms. This poses a daunting challenge that requires concrete responses. Given the fundamental and crucial importance of cooperation of these entities with law enforcement in investigation and prosecution of such offences and in suppressing such misuses, the convention should specify and stipulate obligations and regulations as to the cooperation of the private sector, service providers and other similar entities with law enforcement, in particular sectors and providers with global or substantial outreach at the international level.
- Effective measures for timely and effective cooperation on the part of these entities with law enforcement and judicial authorities should constitute an integral part of the convention. For this purpose, through specific sections within the convention, cooperation between national authorities and entities such as service providers and private sector should be addressed and concrete measures including for expeditious preservation and disclosure of electronic data to law enforcement should be delineated.
- As electronic evidence constitutes a vital element for investigation and prosecution of crimes committed via use of ICT, setting standardized processes for obtaining, maintenance, and disclosure of authentic electronic evidence needs to be among the procedures stipulated in the convention. Standard procedures enable unified and harmonized responses to such crimes at the national level which could also ensure more efficient cooperation among law enforcement and judicial authorities at the international level in relation to the preservation and provision of electronic evidence.
- Recovery and return of assets and proceeds of crime play an important role in depriving criminals of incentives for perpetration of crime and reducing recidivism as well as in providing compensation to victims. Therefore, the expedited seizure, recovery and return of proceeds of crime should constitute a key element of the convention. Relevant provisions of the convention on law enforcement and procedural measures should entrust national authorities with powers that ensure smooth and expedited recovery of assets and proceeds of crimes as well as widest measures of assistance and cooperation in this area.
- The fight against use of ICT for criminal purposes requires that law enforcement be equipped with and use modern technologies in the course of investigation and prosecution of offences in order to proportionately respond to

such crimes. Hence, promoting and supporting the use of modern technology by law enforcement and judicial authorities including throughout procedural measures in preventing and combating crimes committed via ICT should be encouraged. This also necessitates provisions of required equipment and technology to law enforcement and judicial authorities through politically-neutral and reliable technical assistance.

The Islamic Republic of Iran reiterates that adopting a technical approach in elaboration of the convention akin to that taken in elaboration of relevant conventions in the field of preventing and combating crimes which has proved successful and has encouraged many UN Members to sign, ratify or accede to such conventions, should be prioritized.

The Islamic Republic of Iran underlines that realization of a secure cyberspace which promotes moral values and protects human dignity as well as promoting collective international governance in this area based on non-discrimination and with active participation of all states, as a requisite, would ensure an effective fight against the use of ICT for criminal purposes.