

India's Statement on General Provisions:

Thank you Chair,

While technology is neutral in its application, the malicious use of ICTs by criminals has created enormous challenges and threats. The nature of cybercrimes is generally trans-national in nature and the existing investigation and prosecution tools available to Law Enforcement Agencies are quickly becoming outdated. The traditional definition of territorial jurisdiction and existing MLATs are incapable of effectively countering cybercrimes. In view of the above, India proposed in its draft text for a wide scope of application of this Convention; redefining jurisdiction and to build effective international cooperation for sharing of information with safeguards.

Mister Chair,

We have listened carefully to the statements made by the delegations of many member States on General Provisions.

The Indian delegation's views on the twelve guiding questions on General Provisions are as follows:

Q. 1 & 2

Notwithstanding the fact that growth in technology and innovation in cyberspace is too dynamic to easily keep pace with, most of the methodologies/ procedures/ actions/ intent/ outcomes/ impact of the crimes committed through the use of ICTs can be covered through the use of technology neutral terminology. Hence, it is all the more important that the Convention defines crimes committed through the use of ICTs

Additionally, the convention will remain relevant if we use language keeping in consideration the victim, the intention and the action of crime and create a mechanism for broader international cooperation to combat these crimes.

It is well known that traditional crimes committed against natural persons are well defined. If such crimes are committed using ICTs then this convention should cover these crimes for the purpose of enhancing effective and efficient international cooperation among member States.

Q. 3.

The general provisions may be defined on the lines of UNCAC and UNTOC taking into account the unique characteristics of crimes committed through use of ICTs. The main purpose of this Convention is: evidence sharing to enable investigation and prosecution which will result in deterrence, prevention, mitigation and combating of cybercrimes. However, it is most important to bring elements in a technology neutral manner to make

this convention future relevant by bringing in clear and unambiguous enabling clauses for building strong, effective and efficient international cooperation for collection and sharing of non-content and content data to cover all types of crime, be it cybercrimes or traditional crimes while striking a judicious, practical and operational balance between the needs of LEAs and human rights and fundamental rights. This will require modification in the provision on jurisdiction available in UNCAC and UNTOC. India has provided a draft text on jurisdiction to address this issue.

Q4.

The mandate of the UNGA Resolution of this Committee clearly provides the statement of purpose for this Committee in unambiguous manner: The purpose of this convention may be defined as (i) broad terms to combat cybercrimes committed with the use of ICTs (ii) Effective and efficient international cooperation for collection and sharing of information related to cybercrimes (iii) Technical assistance and capacity building with a view to create resilience.

Q5.

The convention is being drafted to counter the criminal uses of ICTs and is not a Human Rights Convention. India supports human rights and fundamental rights. The Convention should include the protection of Human Rights, Fundamental Rights and Privacy Rights of victims of cybercrimes.

Q6

We have listened to member states on this issue. There is wider consensus to provide clear and unambiguous clause or clauses in this convention for sharing of electronic evidence among the member States for all crimes. Sharing of electronic evidence is the prerequisite for combating cybercrimes. This is the soul of this Convention.

India has in its draft text provided a provision on non-content and content information sharing. The non-content information could be shared through nodal agency of each State and content information could be shared through faster mechanism devised by this Convention under MLATs.

The issue of capacity in member States to respond to increased number of requests should not deter or prevent us from providing enhanced, effective and efficient International cooperation. Once this enabling clause is included in the Convention, member States with technical assistance from other member States will upgrade their infrastructure and manpower.

However, the failure to incorporate provisions for international cooperation for collection of sharing of electronic evidence will have catastrophic effects as cybercrimes are

increasing exponentially with large scale impact on the private and public sector, including the developmental goals of member States which directly affects the Fundamental Rights and Human Rights of a large number of the global population.

Q. 7.

Most of the cyber crimes are committed for economic gains. Money is laundered using innovative online means such as the use of crypto-currency. Often, this money movement happens over numerous countries before it is siphoned off by the perpetrators of crimes including cyber terrorists as they are using innovative ways provided by new and emerging technologies to finance terrorist activities. If we are to reign in on cyber crime , we need to cooperate on freezing and return of such proceeds. This will also ensure that the middle man who is operating such laundering channel is also apprehended and prosecuted. India supports freezing, seizure, confiscation and return of the proceeds of such offences.

Q.8.

Article 4 of UNTOC can be a point of reference on defining the issue of sovereignty. However, cybercrime requires parallel and joint investigation in cases where the offence has been committed by multiple actors across many States. Each State then may like to investigate the crime and requires cooperation from member States for collection and sharing of electronic evidence. India has proposed a draft text on Jurisdiction which enables member States to investigate cases that may have multiple jurisdiction.

Q.9

The key terms that require clear and unambiguous definitions are: Computer, ICT, data, computer network, computer system, information, child pornography, child sexual abuse material, proceeds of crime, property, fraud, service provider, sexually explicit conduct, traffic data, content data, cyber crime, confiscation.

Some of the terms have been defined in the Indian draft.

India strongly feels that it is extremely difficult to specify the crime types or types of crimes as technology is continuously evolving and hence new crimes types will emerge which will make this Convention outdated in no time. To address this issue, India proposes that the Convention should have the following:

- (a) It should include crime types – existing and known
- (b) It should include a clause on applicability of this convention to all crimes committed through use of ICTs for international cooperation for collection and sharing of information for investigation and prosecution purposes which are not covered in clause (a).

(c) The crimes not defined in (a) above may be criminalized under this Convention at a later date by member States by adding new protocols to this Convention.

Q 10.

Barring the terms where there is clear consensus, it is most important that member States arrive at the consensus on the following before further defining terms where there is no general consensus:

- (1) Purpose of this Convention,
- (2) Jurisdiction
- (3) International cooperation on collection and sharing of information

Q.11.

Information Communication Technology (ICT) covers any product that will create, store, retrieve, manipulate, transmit, or receive information electronically in a digital form.

Components of ICT are:

- Computer Hardware
- Data
- Software
- Data-Warehouse

Hence, the term 'computer systems' is subsumed in ICT and usage of term "Computer Systems" restricts the scope of the convention drastically whereas the term 'ICT' is broader in scope and sufficiently exhaustive.

Therefore, India affirms that reaching an agreement at the early stage of the negotiation process on the usage of the term 'ICT' is preferable.

Q.12

Technology per se does not discriminate on the basis of gender. However, its malicious use in certain types of crimes disproportionately affects the weakest/ most vulnerable sections of the society, examples being sexual exploitation of women and young girls. Hence the convention should provide faster mechanisms to redress such crimes.
