Comments of the Islamic Republic of Iran in response to the Guiding Questions presented by the Chair of the Ad hoc Committee to Elaborate a Convention on Countering the Use of ICT for Criminal Purposes to the Third Session of the Committee

Agenda Item 4: Provisions on international cooperation
(29 August-9 September 2022-New York)

1. Response to the Questions related to general principles and scope of the provisions on international cooperation

– As regards question number one, we are of the view that international cooperation could include areas such as extradition, law enforcement cooperation, transfer of sentenced persons, transfer of criminal proceedings and electronic evidence, joint investigation, international cooperation for confiscation, and return of assets. Cooperation in these areas, including in conducting the joint investigation would be of important utility in combating criminal acts committed via information and communications technologies which impacts on victims, at times expand across multiple geographical boundaries.

– In addition, taking into account the specific features of such crimes, international cooperation and immediate measures in suppressing the main source of criminal acts and criminal content constitute important areas of cooperation for fighting crimes and minimizing the injury caused by criminal acts.

– As to the question regarding the utility of UNCAC models of extradition and mutual legal assistance, generally, such model could be taken into account; however, the specific features of the crimes in question may require modifications. This remains to be seen for later stages.
On question number four, in accordance with our domestic laws, criminal investigation and prosecution of civil and administrative cases related to the liability of legal persons are not possible.

Our answer to question five is yes, we believe that a threshold penalty period is needed for requesting and granting extradition requests.

On question number six, we are of the view that domestic laws in particular laws concerning procedural powers as well as relevant applicable human rights treaties have already provided sufficient frameworks for respecting human rights. As we have reiterated before, this is not a human rights treaty and the best way forward is to adopt the technical practice taken in the elaboration of UNTOC and UNCAC.

Regarding question number seven, we believe that in the course of judicial investigations concerning criminal cases, access to relevant personal data is necessary, however, protecting the confidentiality of such data should be ensured in international cooperation in this area and states should refrain from disclosing personal data or any other use of the data except for the purpose of investigation, prosecution, and adjudication of the crimes.

2. Response to the Questions related to transmission of requests and materials

For the purpose of extradition, national focal points of states parties could be introduced to the United Nations Office on Drugs and Crime.

For the purpose of facilitating mutual legal assistance, in addition to diplomatic channels, national focal points could also be introduced through a United Nations framework, especially the United Nations Office on Drugs and Crime and in this endeavor, we could also benefit from modern technologies with a view to expediting cooperation and transmit information and electronic evidence in a secure manner.
Likewise, the important role of INTERPOL for facilitating police to police cooperation should also be considered.

- In addition, special mechanisms should be established for cooperation of service providers, entities in the field of domain names and IPs, in particular global service providers and entities, with law enforcement.

- To facilitate international cooperation, establishment of a secure and standard channel of cooperation could be of immense practical utility in fighting crimes committed via ICT. States should have access to such channel without discrimination. To this end, relevant authorities of states could establish 24/7 contact points and standard technical operating procedures as well as a secure platform could be devised for effectively combating these crimes and keep pace with the rate and frequency of crimes committed. Through this platform, where appropriate and necessary, digital tools including electronic signature could be utilized for secure and expedited cooperation. The said features are particularly significant in transfer of electronic evidence which is susceptible to obliteration and modification.

- On question number ten regarding requests for international cooperation, the following elements could be considered as prerequisites:
  - Name and title of the requesting authority
  - Name and title of the requested authority
  - Identity, nationality, occupation, and place of residence or dwellings of defendant/s, plaintiff, victims, the accused, person under trial and convicts.
  - Purpose, subject matter and a summary of relevant facts and description of assistance sought as well as the text of relevant laws
  - The name and address of the receiver, where necessary
  - Reasons and details of a specific procedure or rule which the requested party wants to be observed
▪ Specifying the optimum time-limit for rendering the judicial assistance
▪ Other necessary information for proper rendering of assistance
▪ The documents enclosed with the judicial assistance request should be stamped with the seal of the requesting authority. The requested authority should not object the authenticity and/or validity of such documents.
▪ Other electronic data needed for cooperation such as IP and domain name.

Documents enclosed in requests could also be signed electronically provided that their authenticity is verifiable.

– As regard the extradition, the following information and documents need to be included in the request for extradition:
   ▪ The name of requesting authority
   ▪ The text of the laws and regulations of the requesting states under which the act has been criminalized and the punishment is imposed.
   ▪ Name, surname of the person sought to be extradited as well as his/her father’s name, date of birth, his/her nationality, residence or domicile, identifying marks, photograph, fingerprint and any other information needed, if possible;
   ▪ The details of the crimes for which the extradition has been requested, time and place of commission of the crimes, their legal description and references to the relevant laws and regulations, as far as possible
   ▪ Final conviction, warrant of arrest or summons or any other evidence with the same effect and the period of the sentence which has already been borne, if any.

If the requesting state discerns that it requires any additional clarification is needed, in case the person sought to be extradited is under arrest or under preventive measures, it may
request the requesting stat to provide the required information and determine a deadline for provision of the said information. If the supplementary documents are not received in due time, the requesting state should release the person sought to be extradited. Nevertheless, the above should not preclude further detention of the mentioned person upon receiving the supplementary documents.

− In cases of transfer of sentenced persons, the sentencing state should forward the following documents and information to the enforcing state, unless otherwise agreed between the two states:
  ▪ Identity of sentenced person including name, surname, father’s name, date and place of birth
  ▪ The documents of the nationality of the sentenced person, if any;
  ▪ The text of legal document upon which the judgment is based
  ▪ The request for transfer by the sentenced person or their legal representative or their relatives
  ▪ Documents issued by the sentencing authority or relevant competent authority ascertaining the period of imprisonment served, the detain period before trial, pardon, amnesty or commutation and the remaining period of punishment;
  ▪ Medical documents regarding their physical and mental status

− On question number twelve, we believe that if the channels and networks we earlier mentioned are established, where appropriate, they could be used for cooperation in urgent cases.
3. Response to the Questions related to grounds for refusal

− On question number thirteen, grounds for refusal of extradition should be stipulated in the convention and for this purpose, grounds such as political offenses as well as conflict of request with security, sovereignty and public order should be taken into account as grounds for refusal of extradition.

− On question number fourteen, grounds for refusal of mutual legal assistance should be delineated in the convention. Conflict of request with security, sovereignty and public order should be considered as grounds for refusal of such assistance.

− On question number fifteen, we are of the view that extradition and mutual legal assistance requests could be rejected if they are at variance with the fundamental principles of domestic law; notwithstanding the convention could limit grounds for refusal of cooperation in the following circumstances:
  ▪ Where the accused in a national of the requesting state
  ▪ Where a request for cooperation solely concerns receiving electronic evidence, immediate assistance for the preservation of such evidence and initial investigation
  ▪ Where the request for cooperation is made for the purpose of suppressing the continuation of the crime

− Our response to question sixteen is yes.

4. Response to Other Questions

− Regarding question number seventeen, given the volatile nature of electronic evidence, the convention should lay down provisions that enable provisional measures for the immediate preservation of data. These measures should be made in an expedited manner and maintain
the admissibility and undeniability of the evidence otherwise the evidence may no longer be of utility in criminal proceedings.

– On question number eighteen, we concur with the idea that the convention include investigative powers such as access and real-time collection of data as well as search and seizure of data and computer systems for obtaining electronic evidence. In this context, the responsibility of service providers in data preservation for the purposes of cooperation in investigation and prosecution of the offences, such as user information and content distributed by the person, should also be duly highlighted in the convention.

– On question number nineteen, we believe that given the specific features of the crimes that evade geographical borders, expansion of investigation of criminal cases beyond such boundaries is inevitable yet for this purpose, such cooperation should be conducted through channels of MLA and cooperation. Nevertheless, if the data is publicly available and no particular authorization is needed, like publicly distributed data on internet websites and social networking platforms, law enforcement and judicial authorities could *a fortiori* access such data.

– Accessing data beyond boundaries should be limited to necessary judicial and law enforcement investigation within the scope of crimes in this convention and only in cases where the crime is committed by or against the national of the that state. Such access should be lawful and through public means and not via hacking and similar methods.

– Regarding the second part of the question, it is noted that with the prior explicit consent of the person having lawful authority on the data which are not publicly available, access could be made; provided that such access be lawful and authorized, be within the scope of crimes established in the convention and within the judicial competence of that state, particularly where the crime has been committed by or against the national of that state.
– On question number twenty, highlighting the approach taken in the UNCAC, we would like to reiterate the importance of seizure and return of assets. In this regard, the challenges that in particular, developing countries face in this area should be addressed.

– Previously we have provided our views regarding 24/7 channels of cooperation; such channels should also enable effective cooperation of service providers with law enforcement. In this regard, service providers and other relevant entities including those in the field of domain names, through a 24/7 channel of communication, could respond to and cooperate with law enforcement and judicial authorities in fighting crimes committed via information and communications technologies. These channels and contact points should without discrimination be available to judicial and law enforcement authorities.

– Finally, we believe that hearings could be conducted via video conference and in this relation underline the utility of using information and communications technology by judicial authorities in appropriate cases.